VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky

BAKALÁŘSKÁ PRÁCE

2012 Pavel Zatloukal

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Problematika spolehlivého přenosu dat na digitálních účastnických vedeních

Transmissions reliability with digital subscriber line

2012 Pavel Zatloukal

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Pavel Zatloukal**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Problematika spolehlivého přenosu dat na digitálních účastnických vedeních
Transmissions reliability with digital subscriber line

Zásady pro vypracování:

Pro vysokorychlostní datové přenosy je důležitá spolehlivost. V rámci řešení bakalářské práce navrhněte možné způsoby zabezpečení v laboratorních podmínkách.
1. Úvod do problematiky bezpečných datových přenosů.
2. Návrh možných řešení zabezpečení VDSL2.
3. Ověření funkčnosti v laboratoři.

Seznam doporučené odborné literatury:

Podle pokynů vedoucího diplomové práce.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Pavel Nevlud**

Datum zadání: 19.11.2010

Datum odevzdání: 04.05.2012

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA Fakulta elektrotechniky a informatiky OSTRAVA

prof. RNDr. Vladimír Vašinek, CSc.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení:

„Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal."

V Ostravě dne 4. 5. 2012

Podpis: .....

Poděkování:

Rád bych poděkoval Ing. Pavlu Nevludovi, vedoucímu bakalářské práce, nejen za umožněný stálý přístup do laboratoře N312, ale především za ochotu a odborné vedení, potřebné pro vypracování mé práce.

Abstrakt

Bakalářská práce popisuje návrh a implementaci počítačové sítě pomocí technologie VDSL. Práce se skládá ze dvou částí, a to teoretické a praktické. V teoretické části práce jsou popsány vlastnosti VDSL2, možná rizika ohrožení bezpečnosti sítě a následné návrhy zabezpečení sítě a datových přenosů. Zapojení uživatelů do sítě využívá VLANů, pomocí kterých jsou rozděleni do podsíťových skupin. V praktické části je nejprve uveden návod k vytvoření sítě s prvky VDSL2. Dále je uveden souhrnný popis zabezpečení pomocí OpenVPN, včetně konfigurace obou případných režimů spojení. Při realizaci VPN tunelu mezi dvěma uživateli je detailně otestována propustnost linky šifrovaného a nešifrovaného spojení, a to v závislosti na zvoleném profilu přenosu na zařízení DSLAM. V takto vytvořeném šifrovaném tunelu je následně analyzována činnost přenesených dat při vlivu komprese a zkoumána vytíženost procesoru klientské stanice.

Klíčová slova

VDSL2, OpenVPN, VLAN, DSLAM, zabezpečení, propustnost

Abstract

Bachelor thesis describes the design and implementation of computer network using VDSL technology. The work consists of two parts, namely the theoretical and practical. The theoretical part describes basic characteristics of VDSL2, possible risks to network security and the subsequent proposals of network security and data transmissions. User connectivity to the network utilizes functionality of VLANs, through which are divided into subnetwork groups . The content of practical part contains primarily instructions for setting and configuring a network with elements of VDSL2. In the following part is a hight level description of the security with OpenVPN configuration including two possible connection modes. Following is detailed testing of encrypted and unencrypted chanels of transmission lines. This testing scenario is set up when starting VPN tunnel connection between two users with dependency on the selected transmission profile of the DSLAM. In such an encrypted tunnel is analyzed data status exposed to the influence of compression and CPU utilization at tested client stations.

Key words

VDSL2, OpenVPN, VLAN, DSLAM, security, throughput

Seznam použitých symbolů a zkratek

ACL	**Access Control List**
ATM	**Asynchronous Transfer Mode**
CAP	**Carrierless Amplitude/Phase modulation**
DES	**Data Encryption Standard**
DMT	**Discrete MultiTone**
DoS	**Denial of Service**
DSL	**Digital Subscriber Line**
DSLAM	**Digital Subscriber Line Access Multiplexer**
FDD	**Frequency Divsion Duplex**
FEC	**Forward Error Correction**
FEXT	**Far End Cross Talk**
FTTH	**Fibre To The Home**
HDTV	**High-definition television**
MIMO	**Multiple-input multiple-output**
MTU	**Maximum transmission unit**
NAT	**Network address translation**
NEXT	**Near End Cross Talk**
OFDM	**Orthogonal Frequency Division Multiplexing**
POTS	**Plain Old Telephone Service**
PKI	**Public Key Infrastructure**
QAM	**Quadrature Amlitude Modulation**
QoS	**Quality of Service**
SHA	**Secure Hash Algorithm**
SSL	**Secure Sockets Layer**
TCP/ IP	**Transmission Control Protocol/ Internet Protocol**
TLS	**Transport Layer Security**
UDP	**User Datagram Protocol**
VDMT	**Vectored Discrete MultiTone**
VDSL	**Very High-Speed Digital Subcriber Line**
VoIP	**Voice over Internet Protocol**
VPN	**Virtual Private Network**
WAN	**Wide Area Network**

Obsah

1. Úvod

Bakalářská práce se zabývá návrhem sítě a jejího zabezpečení pro koncové účastníky, a to prostřednictvím širokopásmové sítě VDSL. V návrhu se využívá její druhé generace, která rovněž pracuje na dvoudrátovém metalickém vedení, původně sloužícím pro telefonní služby. Jednou z nejvýznamnějších vlastností technologie VDSL2 je její přenosová rychlost, která se značně zvýšila oproti své předešlé verzi, a to na 100 Mbit/s obousměrného režimu. Těchto velkých rychlostí se dosahuje na velice krátké vzdálenosti, pomocí VDMT modulace a při rozšíření frekvenčního pásma na 30 MHz. Technologie je vhodná mimo jiné na funkce jako triple play, současný provoz telefonních a datových služeb, nebo potřebu symetrického přenosu dat větší přenosovou rychlostí. VDSL využívají existující telefonní kabely, což působí jako alternativa vzhledem k nárůstu optických přípojek, nebo se i uplatňují pomocí společné koexistence s optikou do tzv. hybridních sítí.

V návrhu sítě, zahrnující technologii VDSL2, je využito na přepínači rozdělení stanic do VLANových skupin, které rozdělují síť do seskupení nezávislých na fyzickém uspořádání.

S více se rozvíjejícím světem počítačových technologií, zvyšující se přenosovou rychlostí a rozpínání velikostí internetu, je důležité myslet i na bezpečnost. Žádné zařízení není bezcenné a nejúčinnějším zabezpečením je implementace ochranných prostředků na všech vrstvách. Z důvodu implementace a široké působnosti v oboru informačních technologií je pro daný návrh zvolena forma vybudování virtuální privátní sítě pro zabezpečení datových přenosů. Možností implementace VPN existuje velké množství, a to komerčních i volně dostupných. Pro realizaci bylo zvoleno volně dostupné OpenVPN s širokou podporou platforem a konfiguračních možností. Od verze 2.0 dovoluje OpenVPN využít vedle standardního tunelu mezi klienty i režim server - klient (server - více klientů). V prvním režimu se využívá k šifrování privátní klíč, v druhém je již zabezpečení podstatně rozsáhlejší, a to o asymetrické šifrování s využitím infrastruktury veřejných klíčů zahrnujících výměnu certifikátů podléhající standardu X.509. Takto realizované šifrované spojení, při kterém je možno využít komprese, je náročné na čas určený pro výpočty, a tedy náchylnější na zpomalení rychlosti přenesených dat. Z toho důvodu je nutné nakonfigurované kombinace spojení otestovat a určit, jakou míru zabezpečení je vhodné uplatnit v daném řešení v závislosti na požadované přenosové rychlosti, či vytíženosti procesoru stanice.

2. Teoretická část

2.1. Úvod do technologie xDSL

Systémy xDSL jsou digitální přenosové systémy nasazované na účastnická přípojná vedení. Společným znakem těchto systémů je relativně vysoká přenosová rychlost, řádově až desítky Mbit/s. Využívají položených symetrických párů původně určených pro přenos telefonního signálu. Na vedení jsou nasazovány síťové přípojky místo původního telefonního modemu. Takto sestavená širokopásmová síť je následně zakončena v místní ústředně, nebo rozvaděči mezi ústřednou a účastníkem. Klíčové varianty digitálních přípojek lze rozdělit z pohledu symetrie přenosových směrů (symetrické, asymetrické) a dle metody přenosového kmitočtového (základního, přeloženého) pásma. [13]

2.2. VDSL první generace

Přípojka první generace dosahuje z předchozích modelů rodiny xDSL nejvyšší přenosové rychlosti a koexistuje s přípojkami POTS či ISDN-BRA na jediném vedení. Maximální dosah se předpokládá do 1,6 km, avšak při užití různých vysokorychlostních variant provozu je vzdálenost pouze stovky metrů. V symetrickém režimu má přenosovou rychlost v obou směrech 26 Mbit/s. Oproti tomu v nesymetrickém režimu má rychlost 6,4 Mbit/s vzestupně a 52 Mbit/s pro sestupný směr. Těchto rychlostí se dociluje pomocí modulace DMT s více nosnými, nebo modulací s jednou nosnou v rámci jednoho pásma a to CAP či QAM metodou. Pro obě modulační metody je standardizované přidělení pásem z důvodu kompatibility spektra ADSL, eliminaci přeslechů na blízkém a vzdáleném konci a efektivity pásma vhodného pro přenos. Plán A (označovaný „998“) a plán B (označovaný „997“) užívají dvojí střídání přenosových směrů pásem do 12 MHz.

Pro přenos dat má VDSL v obou směrech přenosu k dispozici prokládaný a neprokládaný kanál využívající bytovou korekci FEC (kód RS). Prokládání při přenosu zaručuje nízkou bitovou chybovost, ovšem za cenu většího časového zpoždění. To je vyžadováno u služeb, které nejsou závislé na komunikaci v reálné čase. [13]

2.3. VDSL druhé generace

VDSL2 je technologií, jejíž standard G.993.2 byl v roce 2006 schválen Mezinárodní Telekomunikační unií, mající za cíl navýšit rychlost od a ke koncovému účastníkovi, a tak být dalším vývojovým stupněm rodinné technologie systémů xDSL. Aby mohla VDSL2 konkurovat a prosadit se v moderním světě kabelových a satelitních systémů, přidává ke svému odběru funkce, jako je triple-play (HDTV, VoIP, Internet) podporovanou vysokou přenosovou rychlostí. Sytém je navržen tak, aby management rozhraní byl totožný jako předchozí systém ADSL2, a díky využití prvků z ADSL má také větší dosah oproti své předešlé verzi a to ideálně až ke 3 km.

Definuje 8 profilů pro specifičtější nároky na regionální konfiguraci. Profil 30a má velkou šířku frekvenčního pásma, na malé vzdálenosti (300 m) dosahuje vysoké přenosové rychlosti a je vhodný do zapojení FTTH. Sestupný směr u profilu 17A má podobný průběh jako 30a, ovšem vzestupný směr je podstatně nižší a volí se tedy do zapojení FTTC. Pro delší smyčky (až 2,5 km) se používá profil 8a, kde se zapojí rovněž do FTTC, nebo častěji do vzdáleného DSLAMu, jak udává Tab. 1.

Profil	8a	8b	8c	8d	12a	12b	17a	30a
Šířka pásma [MHz]	8,5	8,5	8,5	8,5	12	12	17,7	30
Šířka subkanálu [kHz]	4,312	4,312	4,312	4,312	4,312	4,312	4,312	8,625
TX Power [dBm]	+17,5	+20,5	+11,5	+14,5	+14,5	+14,5	+14,5	+14,5
Maximální propustnost [Mbit/s]	50	50	50	50	68	68	100	200

Tab. 1: Parametry VDSL profilů [2]

Šířka frekvenčního pásma byla navýšena z 12 MHz na 30 MHz s možností konfigurace na 8,5 MHz, 12 MHz, 17,7 MHz a 30 MHz. Dále je definován symetrický (Plán „998“) a nesymetrický (Plán „997“) konfigurační plán pro volbu přenosových služeb.

VDSL2 podporuje službu Pre-emption, kdy paket s nízkou prioritou (data) předá přednost paketu s vyšší prioritou (hlas) v jednom kanálu. Dále dokáže přepravovat i pakety menší než 64 B, tedy IP pakety. [2]

2.3.1. Modulace DMT a VDMT

VDSL1 (standard G.993.1) podporuje DMT v hlavní části specifikace a QAM v normativní příloze. Provádí spektrální kompatibilitu se stávajícími službami a pozdější přidávané funkce byly již částí druhé generace VDSL2, stejně jako usnesení na jediném kódování pomocí DMT. [2]
Obě generace systémů používají pro přenos dat na metalických vedeních modulaci s více nosnými DMT, obdobně jako OFDM.

Modulace DMT rozděluje frekvenční pásmo na subkanály s konstantní frekvenční šířkou, kde se provádí modulace uživatelských dat pomocí QAM. Modulace DMT se realizuje pomocí inverzní Fourierovy transformace, kterou se skupina symbolů QAM ve všech subkanálech převede do časové oblasti na tvz. DMT symbol. Vzájemná nezávislost jednotlivých subkanálů dovoluje, podle aktuálního poměru signálu a šumu, používat pro každý subkanál rozdílný počet stavů modulace QAM. Dle Tab. 2 je rozteč subkanálů stanovena na 4,3215 KHz, z důvodu kompatibility účastnických přípojek, vyjma rozšíření pásma u VDSL2 na 30 MHz, kde je dvojnásobná.

Typ přípojky	ADSL2	ADSL2+	VDSL2		
Rozteč subkanálů [kHz]	4,3125	4,3125	4,3125	4,3125	8,625
Počet subkanálů	256	512	1972	4096	3479
Šířka pásma [MHz]	1,1	2,2	8,5	17,7	30

Tab. 2: Subkanály a šířka pásma u digitálních přípojek xDSL [16]

Modulace Vectored DMT je rozšířením předchozí modulace pro skupinu přípojek xDSL. VDMT je navržena na potlačení přeslechu FEXT u přípojky VDSL2, při rozšiřování frekvenčního pásma. Pro správnou funkci vektorové modulace je nutné v DSLAMu provádět pro vzestupný směr kompenzaci přeslechů na přijímací straně a pro směr sestupný předkompenzaci signálu na straně vysílače. VDMT tedy potlačuje nežádoucí přeslechy ve vedení, které vedou k snižování přenosové rychlosti a také řeší problém MIMO více-uživatelského prostředí. [3]

2.3.2. Oddělení kanálů

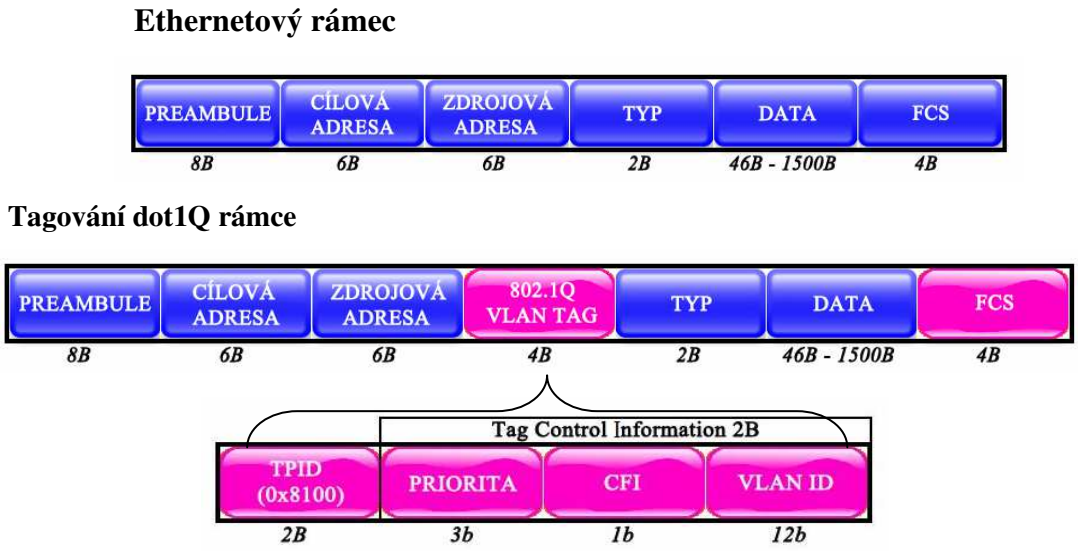
V systémech VDSL se užívá frekvenční dělení kanálů FDD, a to metoda Zipper duplex. Tento systém je koncipován tak, že libovolná dostupná nosná může být použita pro libovolný z obou směrů. Z možného nežádoucího vzájemného prosakování mezi nosnými z důvodu vlastního NEXT přeslechu se předcházelo synchronizací DMT symbolů (doplněním CS a CP k symbolu).

Takto pracující systém je označován za synchronní Zipper duplex. Později se zavedl asynchronní Zipper, u něhož se využívá vhodného tvarování vysílaných DMT symbolů, a to bez nutnosti synchronizace a snížení výkonu vysílaného mimo užité pásmo. [3] [12]

2.3.3. Zapouzdření ethernetového rámce

Běžný ethernetový rámec a následně upravený rámec pomocí tagování dle standardu 802.1q znázorňuje Obr. 1.

Přenos dat je řešen zapouzdřením ethernetového rámce do rámce VDSL. Formát VDSL rámce se skládá z 5 bytové hlavičky a 400 bytů je rozděleno do dvou částí spadající do rychlého a pomalého kanálu.



Obr. 1: Ethernetový rámec a rámec upravený standardem 802.1q [17]

Zapouzdření je transparentní bez manipulace s datovým obsahem a realizuje se odstraněním 8 B preambule z ethernetového rámce a přidělením preambule nové. Takto vytvořený EoVDSL rámec (Obr. 2) je ještě doplněn o prázdné značky obsahující volné byty. [1]

Obr.2: Rámec EoVDSL [1]

2.4. Přístupový multiplexor DSLAM

DSLAM je přístupový multiplexor, který podporuje zapouzdření toku bitů do rámců DSL a paketů pro přenos. Provádí základní monitorování sítě, funkce správy a údržby. [11]
Vedle směrování provozu a distribuce služeb podporuje přenos streaming media a dalších služeb na základě podpory QoS pro spolehlivý přenos aplikací citlivých na zpoždění.

DSLAM ukončuje vedení VDSL2 na straně ústředny. Jeho úkolem je sdružovat provoz od xDSL uživatelů a současně oddělit a následně směrovat hlasový provoz do telefonní sítě a datový do sítě WAN (např. Ethernet, ATM nebo Frame Relay). Přenos dat od uživatelů probíhá v režimu ATM buňkách konstantní délky 53 oktetů, nebo v častějším režimu po IP síti. IP DSLAM pracuje s IP datagramy proměnných délek, podporou více funkcí IP směrovacích protokolů, požadavky moderních služeb a možným přechodem na ATM. [8]

Další formou zabezpečení proti napadajícím stanicím je na úrovni DSLAMu filtrování MAC adres. Tato volba se skrývá v menu ACL (Obr. 8), kde je možnost staticky uvést blokované adresy, povolit naopak jen akceptovaná zařízení, nebo využít výchozího povolení všech stanic.

Pro datový přenos lze do přenosových kanálů nastavit rychlou variantu prokládaní bez přídavného zpoždění, anebo variantu s prokládáním bitů uplatňující vyšší odolnost proti impulsnímu rušení. Zpoždění prokládané cesty závisí na nastaveném parametru hloubky prokládání (Obr.10). Vhodný režim je uplatněn dle okolnosti, zda-li se jedná o přenos služeb citlivých na zpoždění. Přenosové rychlosti jednotlivých kanálů jsou nastaveny během inicializace. [14]

2.4.1. Modem Zyxel

Z portu DSLAMu je dvoudrátem připojen přístroj Zyxel P-870MH-C1. Tento modem/ měrovač druhé generace VDSL systémů se vykazuje přenosovou rychlostí pro vzestupný směr 35 Mbit/s a 65 Mbit/s pro sestupný a je tedy vhodný pro náročné triple-play služby. Zařízení obsahuje 4 LAN porty pro klienty, na něž připojením UTP kabelu přidělí stanici IP adresu z rozsahu nastavených adres.
Z VDSL2 profilů, které popisuje Tab. 1, podporuje 8a, 8b, 8c, 8d, a 12a profil. [19]

Obr. 3 –Používaný Modem a DSLAM technologie VDSL2 [19]

2.5. Zabezpečení sítě

2.5.1. Úvod a druhy útoků

Žádné zařízení připojené k internetu není pro potenciální útok bezcenné a ohrožení komunikačního systému může zahrnovat zničení, poškození, modifikaci i ukradení informací, či přerušení služeb například formou velkého množství útoků (DoS). Nejčastější útoky jsou reprezentovány maskováním (vydáváním za někoho jiného), změnou práv, nebo použitím „trojského koně“. [10]

Další formy útoků jsou zjišťování nešifrovaných informací odposlechem po síti, realizované počítačem s vhodným softwarem. Typ útoku „man-in-the-middle“ představuje situaci, kdy falešný certifikát serveru je poslán klientovi – ten jej bez ověření přijme a následně může dojít k zjištění údajů, či hesel. [4]

2.5.2. Bezpečnostní technologie

Bezpečnost sítě má mnoho stránek a různých úhlů pohledu na potenciální hrozbu sítě. Nejlepší a zároveň mnohdy nejčastější je návrh vrstvené bezpečnosti, za kterou můžeme považovat síť, jejíž alespoň elementární zabezpečení je implementováno na všech stávajících částech.

Z pohledu 3. vrstvy modelu TCP/IP tvoří na směrovači obrannou linii paketové filtry ACL, které filtrují pakety podle zdrojové a cílové adresy. Tyto filtry se dále kombinují s firewallovými technologiemi jako stavová inspekce paketů SPI, pracující na 4. vrstvě a sledující stav spojení TCP. Další vrstvu zabezpečení představuje překlad sítových adres NAT, jehož hlavním úkolem není jen vyřešit nedostatek veřejných IP adres, ale výrazně ztížit mapování topologie sítě, údaje o konektivitě a informací počtu počítačů v síti. [15]

2.5.3. Bezpečnostní kódy

Zabezpečení přenosu digitálního signálu proti chybám lze zajistit různými způsoby. U přípojek xDSL nejsou vhodné použitelné metody, které spočívají v opakování části zprávy. Vzniká při nichž značné zpoždění, což je nepřípustné pro přenos aplikací v reálném čase. Jedná se o kódy, zavádějící do vysílané části dat předdefinované zákonitosti, kde jejich porušení značí chybu. Jejich zavedení většinou znamená rozšíření zprávy o kontrolní prvky. Rozdělit kódy lze na detekční a korekční.

Vzhledem k dalšímu rozdělení se u xDSL systémů používají systematické blokové kódy. Korekční mechanismus (FEC) vyjadřuje, že data jsou nejprve před přenosem kódovány pro následnou opravu v přijímači. [13]

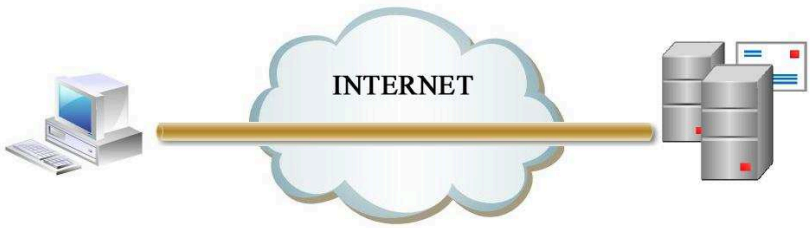
2.5.4. VLANy

Virtuální LAN slouží k logickému rozdělení sítě nezávisle na fyzickém uspořádání. Pomocí VLAN lze vytvořit dvě sítě na jednom přepínači, což by muselo být dříve realizováno na dvou přepínačích apod. Při realizaci více VLANů na jednom přepínači je komunikace zasílána pouze na porty spadající do patřičné VLANy. Pokud není definováno, veškeré porty přepínače spadají do výchozí VLAN 1. Zařazení do VLANy lze podle MAC adresy, podle protokolu, podle autentizace, nebo nejčastěji ruční konfigurací podle portu přepínače. Z důvodu komunikace mezi různými výrobci přepínačů byl stanoven standard IEEE 802.1q, který využívá značkování (tagování) rámců. Princip tagování rámců je, že se ethernet rámec doplní o 4B informaci „dot1Q“ tagu viz rámec na Obr. 1. Vložena je informace protokolu 802.1q (hodnota 0x8100), priorita protokolu 802.1p, normativní ukazatel a ID číslo VLANy. Při komunikaci mezi dvěma zařízeními se využívá trunk portu, který přenáší jakýkoli VLAN. [17]

2.6. Virtuální privátní síť

Virtuální privátní sítě neboli VPN je metoda, s jejíž pomocí je umožněn přístup do vnitřní (podnikové, domácí apod.) sítě ze sítě vnější. Jedná se o propojení počítačů rozložených po celém internetu a vytvoření tzv. virtuální sítě. Zařízení skutečně vypadají, jako by byly skutečně spojené i s výhodami, které z toho plynou.

Obr. 4 zobrazuje modelovou situaci spojení klienta (klientů) k serveru s veřejnou IP adresou. Po připojení klienta obě strany vytvoří šifrovaný kanál (tunel). Po autentizaci klienta je mu přidělena IP adresa a klient se stává součástí sítě. Klientské připojení k internetu je užíváno už jen pro využívání šifrovaného kanálu. [4]



Obr.4: Realizace VPN

2.7. OpenVPN

Systém OpenVPN je otevřená implementace VPN, která je šířená pod licencí GNU/GPL. OpenVPN je nezávislá na platformě a lze ji provozovat na systémech Windows, Linux, Mac OS X, Solaris, FreeBDS a NetBDS a běží v uživatelském režimu bez potřeby úpravy jádra. Nabízí široké možnosti konfigurace zabezpečení s použitím TLS/SSL a volitelné komprese dat. Autentizace komunikujících stran probíhá pomocí statického klíče nebo pomocí PKI s certifikáty odpovídající standardu X.509. Spojení probíhá na protokolu UDP/TCP, kde dochází k vytvoření virtuální síťové karty, reprezentující virtuální spojení s druhou stranou zařízení v síti. Způsoby vytvoření komunikace je pomocí jednoduššího tunelu mezi dvěma klienty, nebo konfigurace plnohodnotné virtuální sítě server - klient. Výhodou této komunikace je použití jednoho předem dohodnutého portu. [4]

2.7.1. Šifrovací algoritmy

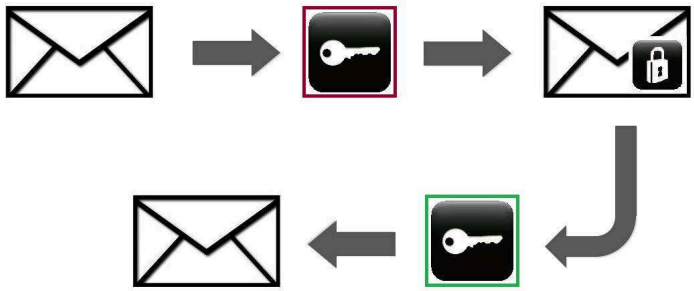
Stanice, které si chtějí šifrovat svá data při komunikaci, zpravidla využijí jednoho, nebo kombinaci dvou typů přístupu k šifrování. Šifrování soukromým klíčem využívá tvz. privátní klíč, který vlastní komunikující uživatelé. Šifrování i dešifrování se provádí stejným klíčem a jedná se tedy o symetrické šifrování, obvykle nenáročnějšími algoritmy na výpočet např. DES.

Obr. 5: Průběh symetrického šifrování

Naproti tomu asymetrické šifrování, tedy pomocí veřejného klíče, je zdaleka bezpečnější metodou. Zapotřebí jsou dva klíče, z nichž jeden je soukromý a druhý veřejný. Jestliže uživatel A chce zaslat uživateli B zašifrovanou zprávu, musí použít k zašifrování veřejný klíč, který mu poslal uživatel B přes nezabezpečenou síť. Uživatel B poté dešifruje zprávu svým soukromým klíčem. V situaci, kdy dojde k odchycení veřejného klíče při výměně mezi uživateli, nedokáže útočník komunikaci rozšifrovat ani při znalosti veřejného klíče, algoritmu, přenášené zprávy, neboť mu chybí potřebný privátní klíč příjemce.

Pro bezpečnost lze zprávu ještě zašifrovat privátním klíčem uživatele A a následné dešifrování provede uživatel B pomocí veřejného klíče uživatele A. Šifrování privátním klíčem je používáno pro

digitální podpis odesílatele, který podepíše - zašifruje vygenerovaný hash kód zprávy. Příjemce ověří certifikát a při porovnání hash kódů zjistí, zda-li nedošlo k modifikaci zprávy. [10]



Obr. 6: Průběh asymetrického šifrování

2.7.2. Protokol TLS s infrastrukturou veřejných klíčů

Kryptografická vrstva OpenVPN využívá dvou autentizačních režimů. Pomocí předem sdíleného statického klíče, nebo užití SSL/TLS a certifikátů pro ověřování a výměnu klíčů.

V režimu statického klíče se využívá symetrického šifrování, tedy klíč je vygenerován před vznikem tunelu. Statický klíč obsahuje 4 nezávislé klíče (HMAC pro odesílaní, HMAC pro příjem, šifrování a dešifrování), které jsou na obou koncích totožné.

SSL/TLS režim je založen na obousměrné autentizaci. Zda-li je splněna, tak jsou náhodně zvoleny bezpečnostní mechanizmy. Při užití klíčové metody 1 jsou klíče generovány z OpenSSL RAND_bytes funkce. Ve verzi OpenVPN 2.0 je výchozí klíčová metoda 2, která využívá pro generování TLS PRF. Spojení začne, jakmile je dohodnutá sada obou podporovaných klíčů. Blowfish je výchozí šifra a SHA1 je výběr pro zprávy. OpenVPN poskytuje SSL/TSL spojení na spolehlivé transportní vrstvě pomocí zvolených UDP nebo TCP paketů. Podrobnější popis problematiky je nad rámec této práce. Zachycený provoz je uveden v Příloze 3. [7]

2.7.3. Lempel–Ziv–Oberhumer komprese

LZO je kvalitní, platformě přenositelná, bezztrátová komprese dat. Tato knihovna je určena pro kompresi a dekompresi dat v reálném čase. Je vhodná pro vysokorychlostní služby, jelikož upřednostňuje rychlost před kompresním poměrem. Kompresní algoritmy vyžadují 64 kB paměti, nebo i úroveň komprese pomocí 8 kB. Na rozdíl od dekomprese nepotřebující žádné místo v paměti. Komprese a dekomprese dat probíhá v rámci stejně velkých bloků kódu. [5]

3. Praktická část

3.1. Schéma návrhu sítě

Návrh sítě zahrnuje přepínač, na kterém jsou nastaveny VLANové skupiny a trunk linkou připojen směrovač a DSLAM. Konfigurační stanici je zvolena IP adresa, nezbytná pro vstup do nastavení přístupového multiplexoru. Podstatnou částí ve Schématu 1 jsou klientské stanice PC 9 a PC 8, sloužící pro zastoupení klientů patřících do různých sítí, na kterých se realizuje odpovídající zabezpečení a testování spojení. Klient je UTP kabelem připojen do modemu a následně z VDSL modemu vyveden dvoudrátovým kabelem koncovky RJ-11 do nakonfigurovaného portu DSLAMu. Stanice PC 7 nevyužívá VDSL spojení a je začleněna do návrhu z důvodu testování přenosových rychlostí vzhledem k VDSL klientům.

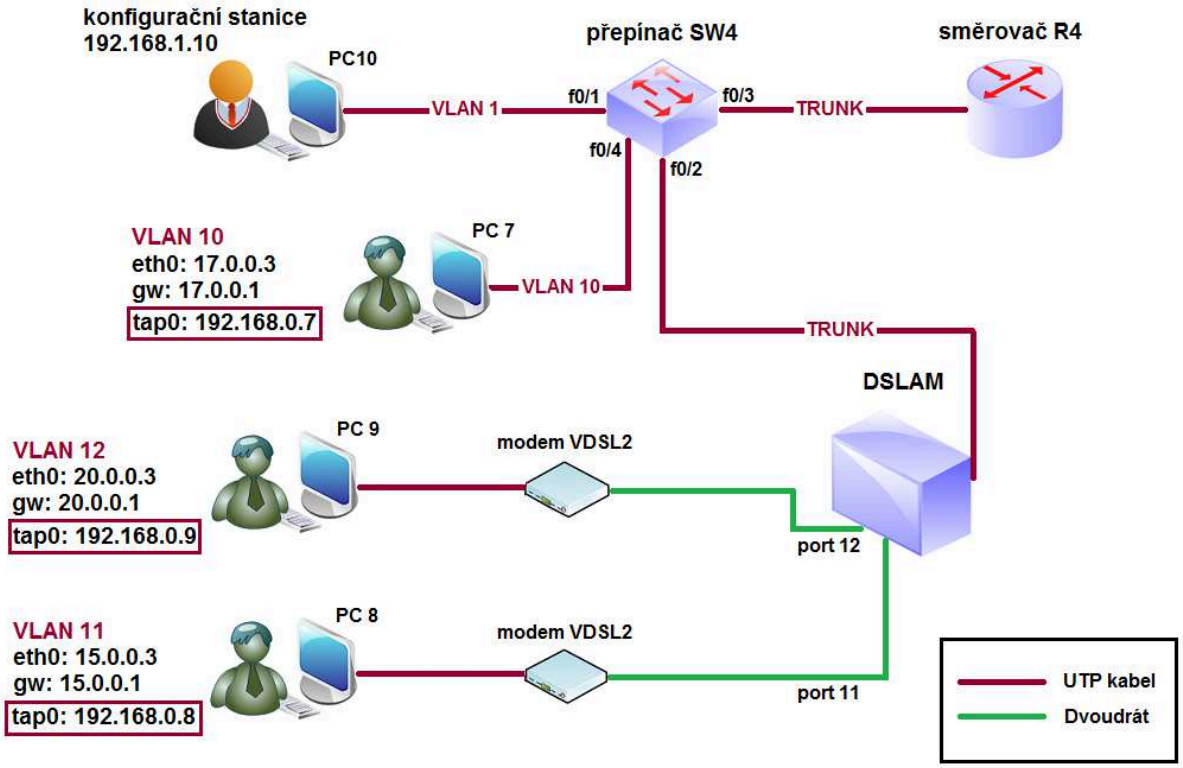


Schéma 1: Návrh sítě

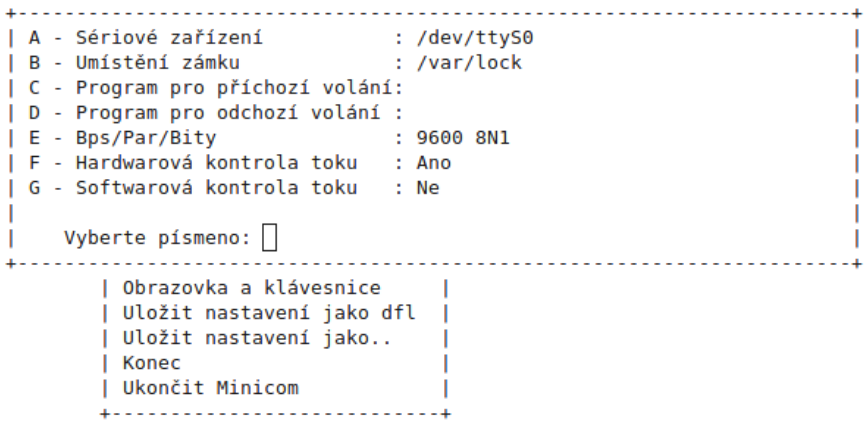
3.1.1. Použité přístroje a prvky

V návrhu jsou použity následující síťové prvky:

- DSLAM Zyxel IES-5005 obsahující: Management Switch Card MSC1000G
  VDSL Line Card VLC1224G-41
- Směrovač Cisco 2800 Series
- Přepínač Cisco 2960 Series
- VDSL modem Zyxel P-870MH-C1

3.2. Konfigurace sítě pomocí VLAN

Pro konfiguraci přepínače a směrovače slouží prostřednictvím sériové linky program Minicom. Po propojení aktivního prvku konzolovým kabelem v příkazovém řádku zadáme *minicom –s,* kterým se dostane do menu a dále je potřeba nastavit odpovídající parametry. Sériový port je značen v sytému Linux *S0* v MS Windows *COM1* a rychlost spojení je zvolena na *9600* B/s.



Obr. 7: Nastavení Minicomu

Takovéto nastavení je poté uloženo jako výchozí.

Při "zamčení" sériového portu způsobeného např. odpojením přístroje je pro jeho odemčení zapotřebí v příkazovém řádku akce: *#rm /var/lock/LCK..ttyS0*

3.2.1. Konfigurace přepínače SW4

```
SWITCH>enable                          // přechod z uživatelského do privilegovaného režimu
SWITCH#configure terminal              // přechod do konfiguračního režimu
SWITCH(config)#hostname sw4            // název zařízení

sw4(config)#interface fastEthertnet 0/4        // přepnutí do konfigurace rozhraní
sw4(config-if)#switchport mode access          // nastavení portu do přístupového módu
sw4(config-if)#switchport access vlan 10       // zařazení do VLANy 10
sw4(config-if)#no shutdown                     // zapnutí portu
sw4(config-if)#exit                            // přechod do nižšího režimu

sw4(config)#interface range fastEthernet 0/2
sw4(config-if)#switchport mode trunk                  // nastavení portu do TRUNK modu
sw4(config-if)#switchport trunk allowed vlan all      // povolení všech VLAN
sw4(config-if)#no shutdown
sw4(config-if)#exit

sw4(config)#interface range fastEthernet 0/3
sw4(config-if)#switchport mode trunk
sw4(config-if)#switchport trunk allowed vlan all
sw4(config-if)#no shutdown
sw4(config-if)#exit                            // zpět do konfiguračního módu
sw4(config-if)#exit                            //zpět do privilegovaného režimu
sw4#
```

Pro ověření správné konfigurace přepínače slouží v privilegovaném režimu pro výpis akce:
#show running-config, #show interfaces a nebo #show vlan.
[18]

3.2.2. Konfigurace směrovače R3

```
ROUTER>enable                                          // přepnutí do privilegovaného modu
ROUTER #configure terminal                             // přepnutí do konfiguračního módu
ROUTER (config)#hostname r3

r3(config)#interface fastEthernet 0/0.4                // přepnutí do konfigurace rozhraní
r3(config-subif)#encapsulation dot1Q 10                // číslo VLANy dle 802.1q
r3(config-subif)#ip address 192.168.1.2 255.255.255.0  // nastavení ip adresy
r3(config-subif)#no shutdown                           // zapnutí portu
r3(config-subif)#exit

r3(config)#interface fastEthernet 0/0.11
r3(config-subif)#encapsulation dot1Q 11
r3(config-subif)#ip address 15.0.0.1 255.255.255.0
r3(config-subif)#no shutdown
r3(config-subif)#exit

r3(config)#interface fastEthernet 0/0.12
r3(config-subif)#encapsulation dot1Q 12
r3(config-subif)#ip address 20.0.0.1 255.255.255.0
r3(config-subif)#no shutdown
r3(config-subif)#exit

r3(config)#interface fastEthernet 0/0
r3(config-subif)#no shutdown
r3(config-subif)#exit                                  // zpět do globální konfigurace

r3(config)#exit                                        // zpět do privilegovaného modu
r3(config)#end                                         // ukončení konfigurace směrovače
```

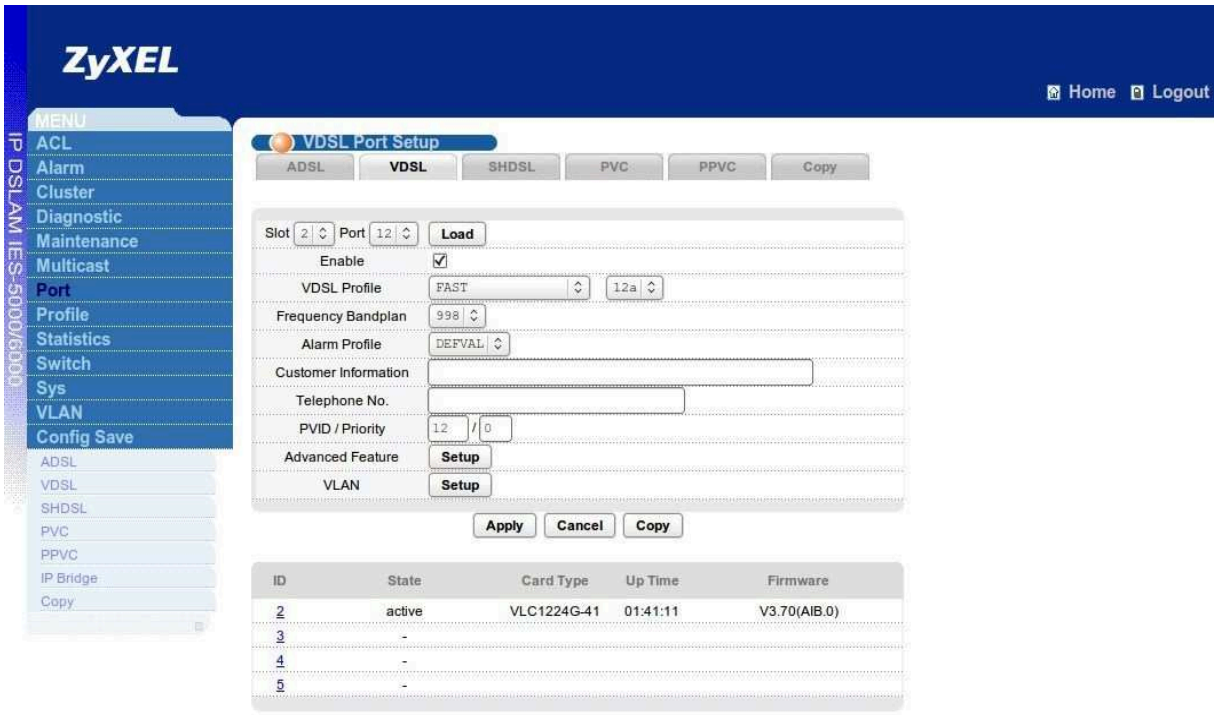
[18]

3.2.3. Nastavení DSLAMu a modemů VDSL2

Pro konfiguraci DSLAMu je možno využít na učebně N312 vyvedeného portu v racku A pro konzolový vstup. Uživatelsky přívětivější je ovšem vstup pomocí webového prohlížeče na konfigurační stanici. Na stanici je do webového prohlížeče zadána IP adresa DSLAMu 192.168.1.1. Přístup je možný pouze ze stejné podsítě a stanice tedy musí mít např. adresu 192.168.1.10.
Pro přihlášení do menu slouží výchozí údaje: *admin*

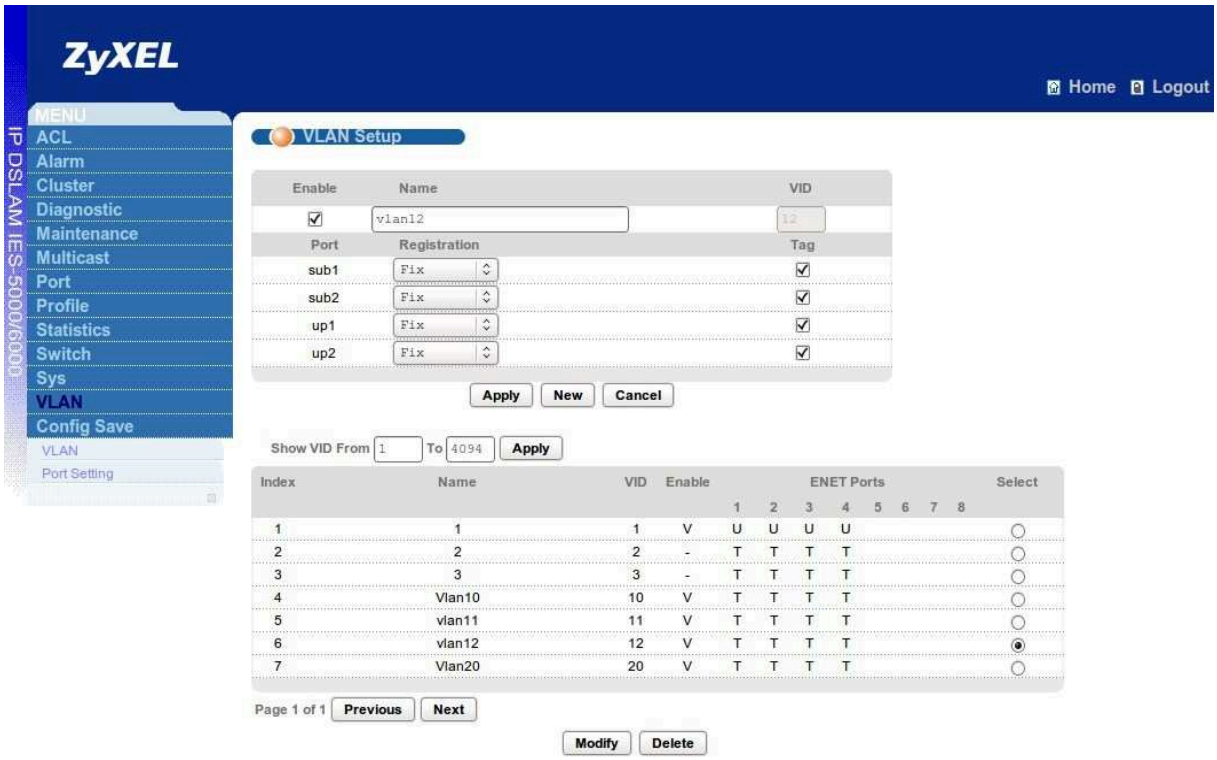
1234

Po zdárném přihlášení už je možno provádět změny v nastavení a potřebné administrátorské funkce. Významná je záložka *Port* (Obr. 8), která se užívá pro správnou funkci portů a udává možnost konfigurace jejich VDSL profilu, VLANy, frekvenčního plánu, nebo priority. Tyto volby spojení musí být měněny shodně na komunikujících stanicích. Konkrétně je použit plán 998 vhodný pro asymetrické služby, FAST profil a frekvenční profil 12a, jehož popis je uveden v Tab. 1 na str.3. Port 12 DSLAMu spadá do VLANy 12 a rovněž analogicky spadá i port 11 do VLANy 11.



Obr. 8: Menu pro výběr portu

Obr. 9 zachycuje náhled záložky *VLAN*, kde je 12 VID povolena a zobrazen souhrnný přehled. Značka „T“ vyjadřuje navolené tagování a „U“ značí netagovaný port.



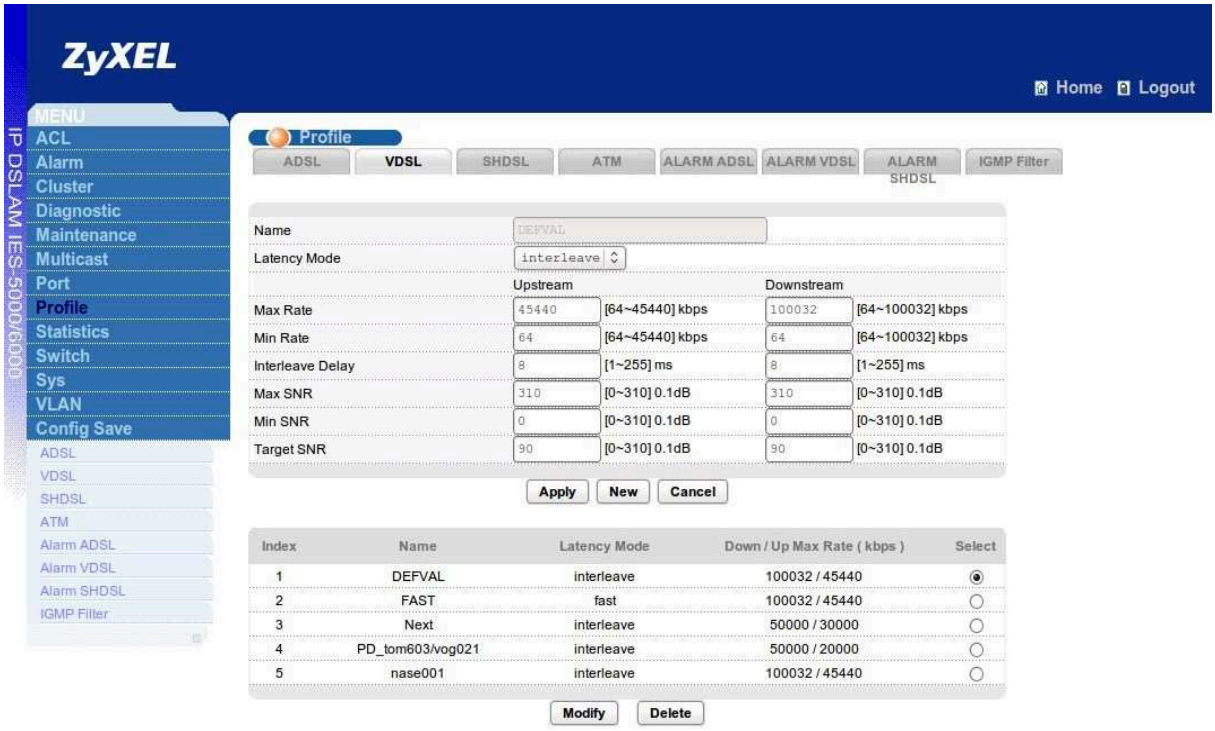
Obr. 9: Menu nastavení VLAN skupin

Záložka *Profile* obsahuje možnost editace, popř. vytvoření nového profilu obsahující základní nastavení, jako je rychlost přenosových dat, chybovost, mód latence a jiné.

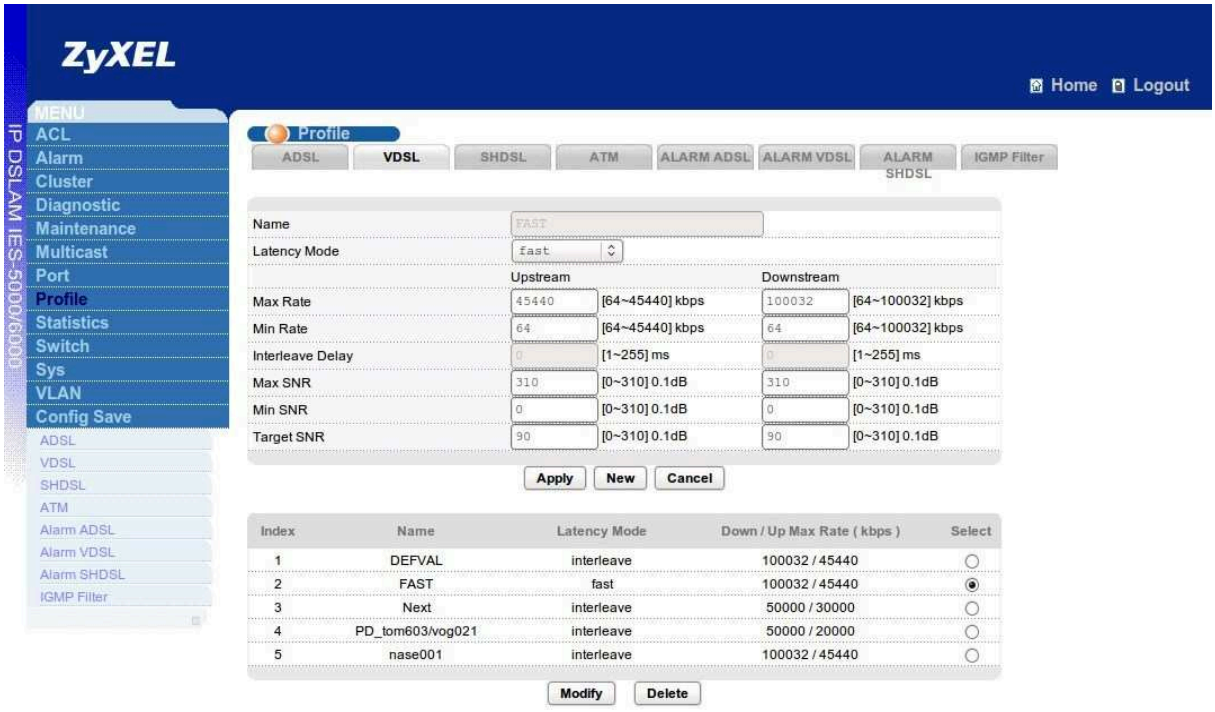
V návrhu bylo využito profilu DEFVAL, který je výchozím profilem s latencí prokládání bitů. Profil má nastavené maximální rychlosti pro přenos dat, což je pro sestupný směr 100 Mbit/s a vzestupný směr 45,5 Mbit/s.

Dále byl vytvořen FAST profil s totožnými hodnotami přenosových rychlostí jako u předchozího profilu, ovšem bez možnosti prokládání bitů. Na těchto dvou VDSL profilech je aplikováno VPN zabezpečení a následně provedeno otestování maximální propustnosti spojení v kombinacích s šifrovaným přenosem i v závislosti na kompresi. To z důvodu případného omezení kvality spojení, závislém na zpoždění při prokládání bitů.

Podrobnější náhledy nastavení profilů zobrazuje Obr. 10 a Obr. 11 na straně 17.



Obr. 10: Profil DEFVAL s prokládaným módem latence



Obr. 11: Profil FAST s rychlým módem latence

3.3. OpenVPN mód tunel mezi klienty

Pro vytvoření šifrovaného tunelu je třeba, aby obě klientské stanice měli veřejnou IP adresu. Obě strany budou vlastnit shodný vygenerovaný klíč, potřený k autorizaci a šifrování/dešifrování zpráv. [4]

3.3.1. Konfigurace klientských stanic

K vytvoření VPN spojení je nejprve nutná instalace OpenVPN na každé stanici. Pod systémem Linux spustíme terminál a přihlásíme se jako *root*. Pro instalaci je nutné napsat do příkazové řádky příkaz:

apt-get install openvpn

Tímto příkazem se nainstalovalo OpenVPN na stanici včetně potřebných knihoven, např. knihovny LZO pro kompresi dat.

Pro vygenerování sdíleného klíče na stanici PC9 lze použit příkaz:

openvpn –genkey –secret /etc/openvpn/secret.key

Takto vytvořený klíč z náhodných hodnot je nutno dopravit bezpečnou cestou na stanici PC8.

Na klientské stanici PC9 bude v souboru *vpn.conf:*

remote 20.0.0.3	# IP adresa druhé strany
ifconfig 192.168.0.9 255.255.255.0	# adresa virtuálního zařízení
port 5001	# zvolený port
proto udp	# komunikace pomocí UDP
dev tap0	# typ a číslo virtuálního zařízení
secret /tec/openvpn/secret.key	# umístění sdíleného klíče
ping 10	# interval keep-alive pingů
comp-lzo	# zapnutí komprese LZO
verb 5	# četnost informovanosti od 0-11
mute 10	# tlumení záznamů
#user openvpn	# uživatel
#group openvpn	# skupina

Na klientské stanici PC8 bude rovněž *vpn.conf* soubor se stejnou konfigurací, ovšem s odlišnými adresami:

remote 15.0.0.3

ifconfig 192.168.0.8 255.255.255.0

…

Tyto soubory musí být uloženy v adresáři */etc/openvpn/* společně s vygenerovaným klíčem *secret.key*. Nainstalované skripty v adresáři pro všechny konfigurační soubory spustí démona. Spuštení VPN provedeme příkazem: */etc/init.d/openvpn start*

Analogicky zadáme totožný příkaz s koncovým slovem *stop* pro ukončení VPN spojení. Koncovou modifikací *restart* opětovně zprovozní VPN, například při změně v konfiguračních souborech. Zda-li je potřeba monitorovat dané VPN spojení, pak k tomu slouží příkaz, vypisující stav četností parametru *verb*: *openvpn --config /etc/openvpn/vpn.conf*

Takto vytvořené spojení mezi stanicemi vytvoří tunel mezi virtuálními rozhranními tap0na druhé vrstvě TCP/IP, na jejichž adresu jsou veškerá data šifrována vygenerovaným klíčem. Výpis spojení zobrazuje Obr. 1 v Příloze 1. Pro přehled je v Tab. 4 uveden souhrn potřebných souborů pro tuto konfiguraci včetně umístění a funkce souborů. [4]

Soubor	Umístění	Funkce	Tajný
vpn.conf	Oba klienti	Konfigurační soubor	NE
secret.key	Oba klienti	Vygenerovaný klíč	ANO

Tab. 4: Přehled souborů pro konfiguraci [6]

3.4. Měření propustnosti linky

Pro zjištění maximální propustnosti linky byl použit program Iperf. Tento program lze jednoduše obsluhovat pomocí příkazů z terminálu, nebo lze využít grafického rozhranní s názvem Jperf. Podpora JAVY na počítačích v učebně N312 chybí a je tedy využito prvně zmíněného. Iperf dokáže otestovat propustnost od klienta na server, kterou omezuje pouze hardwarové řešení. Na učebně N312 je již při spuštění počítače nainstalován, ovšem nezbytně se zadá do terminálu příkaz:

apt-get install iperf

Dostupné funkce se zobrazí pomocí nápovědy zadáním *iperf –h.* K samotnému otestování je nutné, aby jedna stanice byla ve funkci serveru (parametr *-s*) a vyčkávala následnému připojení klienta (parametr *–p IP_adresa_serveru*).

K průběhu přenosu lze specifikovat čas k přenášení dat (*-t počet_sekund*), četnost stavu výpisu (*-i počet_sekund*), velikost MTU (*-m*), použití vlastního portu (*-p port*), obousměrný režim přenosu (*-d*), vlastní velikost MTU *(-M velikost*) atd. Náhled z výpisu programu je uveden v Příloze 2.

3.4.1. Výchozí propustnost linky

Před samotným měřením propustnosti byla vytvořena síť oddělená dvěma směrovači z důvodu ověření výchozí propustnosti bez vlivu VDSL2. Dle Schématu 2 vznikly dvě oddělené sítě symbolizující reálný provoz, které byly potřebné k získání veřejných adres k realizaci VPN tunelu mezi
stanicemi.

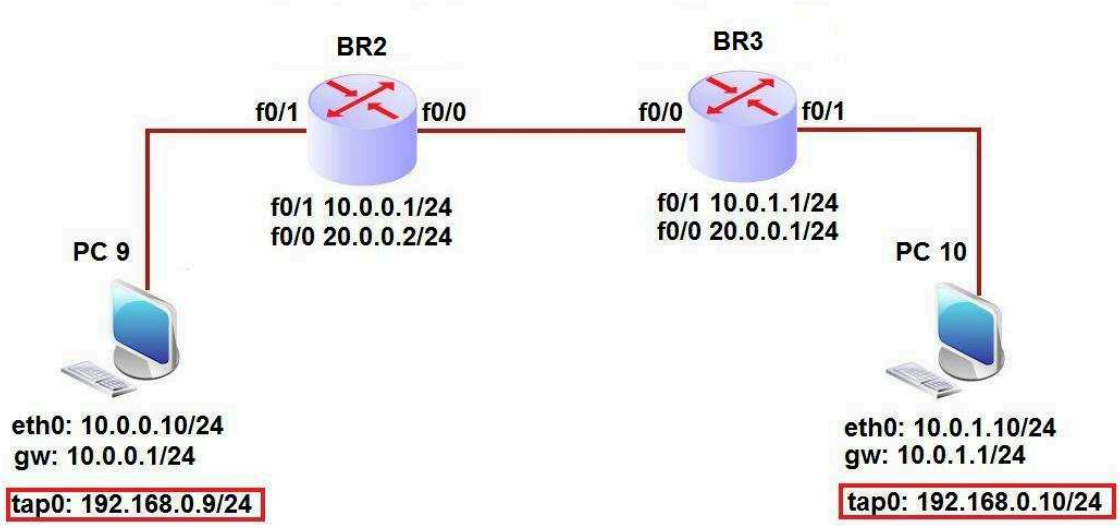


Schéma 2: Výchozí propustnost linky

Nakonfigurované adresy jsou uvedeny u aktivních prvků. Dále je nutné na obou stanicích kvůli směrování definovat adresu výchozí brány fast ethernetu na nejbližším směrovači.
Na směrovači je ještě nutno přidat statické směrování protější adresy f0/0 směrovače. Příkladně na BR3 příkazem a analogicky totéž na BR2:
ip route 0.0.0.0 0.0.0.0 20.0.0.2
Programem Iperf byla následně otestována propustnost linky (Tab. 3) na nešifrované rozhraní eth0 a poté na virtuálním rozhraní tap0, které šifruje pomocí vygenerovaného klíče.
Tabulka zobrazuje naměřené rychlosti daných rozhraní, a to v kombinaci jednosměrného a obousměrného současného přenosu dat.

		Propustnost [Mbit/s]	MTU [Byte]
Nešifrovaný	Jednostranný	**95**	1500
	Oboustranný	80	1500
		89	1500
OpenVPN s LZO kompresí	Jednostranný	**84**	1361
	Oboustranný	45	1361
		37	1361
OpenVPN bez komprese	Jednostranný	**68**	1362
	Oboustranný	36	1362
		34	1362

Tab. 3: Výchozí propustnost linky

3.4.2. Propustnost linky mezi VDSL klienty

Hodnoty uvedené v Tab. 4, vyjadřují maximální rychlost přenosu dat po lince. Propustnost byla otestována mezi VDSL klienty (PC 9 a PC 8). Nešifrovaným přenosem je myšleno měření zasílání dat na ethernetové zařízení eth0, tedy přenos bez VPN spojení. Jednostranné spojení je spojení měřené programem Iperf po jednom portu ze strany klienta na server. Oboustranný režim je přenos dat z obou směrů po vlastním samostatném portu stanice.

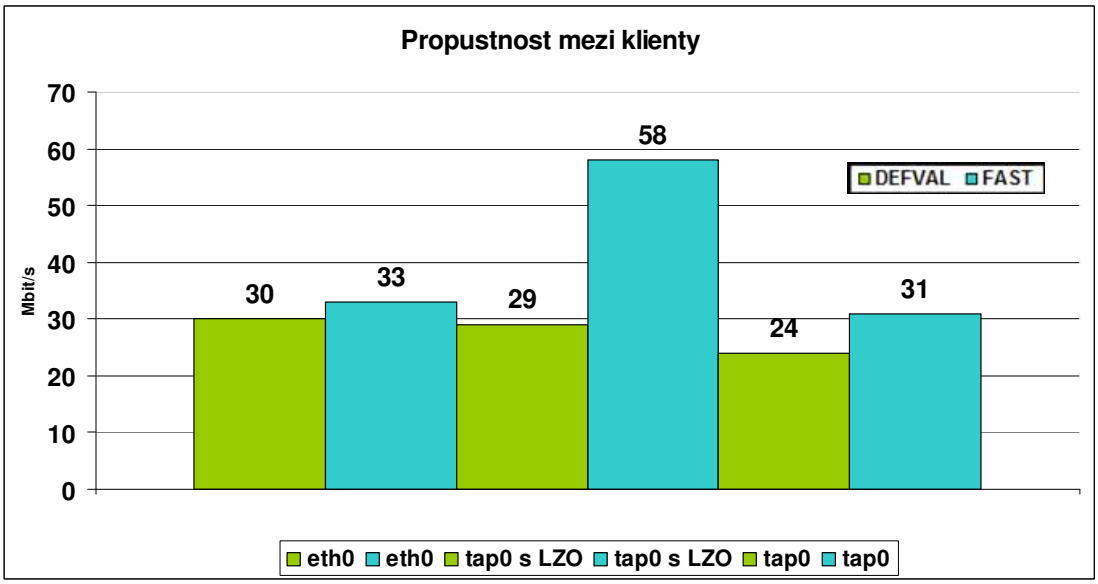
		DEFVAL [Mbit/s]	FAST [Mbit/s]	MTU [Byte]
Nešifrovaný	Jednostranný	**30**	**33**	1500
	Oboustranný	24	28	1500
		20	27	1500
OpenVPN s LZO kompresí	Jednostranný	**29**	**58**	1361
	Oboustranný	17	31	1361
		16	30	1361
OpenVPN bez komprese	Jednostranný	**24**	**31**	1362
	Oboustranný	15	19	1362
		15	20	1362

Tab. 4: Naměřené hodnoty propustnosti linky

Průměrné jednostranné hodnoty rychlostí na lince se pohybovaly kolem 30 Mbit za sekundu u obou profilů nastavených na přístupovém multiplexoru DSLAM. Ovšem FAST profil, který ve svém

přenosu neprokládá bity vykazuje u VPN tunelu s kompresí vynikající rychlost 58 Mbit za sekundu. Přehlednější průběh udává i Graf 1.

Pro oboustranný směr přenosu měli stanice tendenci vyrovnávat svoji přenosovou rychlost. V daných kombinacích je uvedena i velikost maximální přenosové jednotky MTU.



Graf 1: Propustnost linky pro jednostranný směr přenosu

Pro detailnější rozbor problematiky bylo realizováno spojení mezi klientem využívající VDSL technologii a „běžným“ klientem (PC 7) připojeným přímo do přepínače. Takto vytvořená síť byla otestována shodně dle předchozího měření jako u VDSL klientů.

Hodnoty jsou přehledně zobrazeny ve formě tabulky a opět je měřena propustnost šifrovaných VPN přenosů a i mezi ethernetovými zařízeními. Tab. 5 udává v horní polovině propustnost směrem od PC 9 na PC 7 a ve spodní části tabulky naopak. Toto rozdělení je z důvodu různých naměřených přenosových rychlostí. Rozdíly jsou dány měřeným směrem propustnosti programu Iperf, kde se jedná o směr od klienta na server.

			DEFVAL [Mbit/s]	FAST [Mbit/s]	MTU [Byte]
Propustnost od VDSL klienta na PC7	**Nešifrovaný**	Jednostranný	**32**	**33**	1500
		Oboustranný	8	11	1500
			55	56	1500
	Šifrovaný OpenVPN	Jednostranný	**40**	**69**	1361
		Oboustranný	24	36	1361
			20	33	1361
Propustnost od PC7 na VDSL klienta	**Nešifrovaný**	Jednostranný	**56**	**56**	1500
		Oboustranný	54	56	1500
			9	11	1500
	Šifrovaný OpenVPN	Jednostranný	**38**	**66**	1361
		Oboustranný	19	34	1361
			23	34	1361

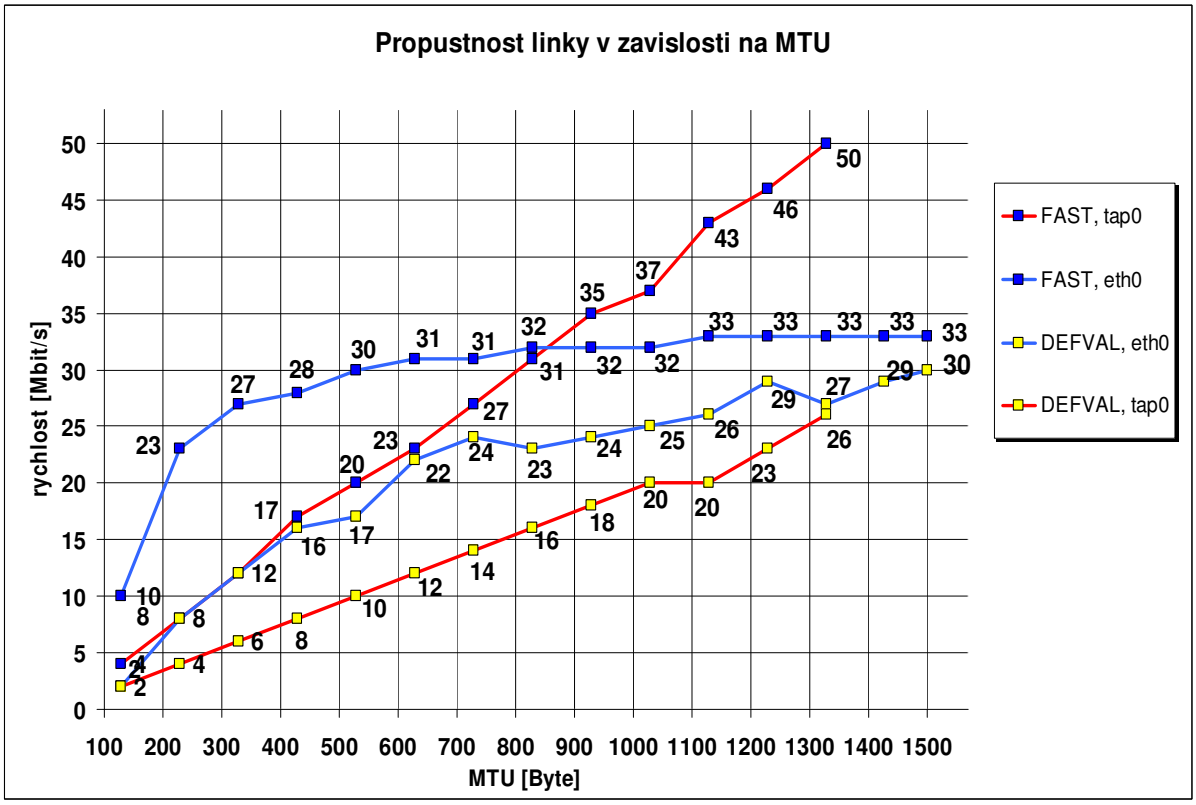
Tab. 5: Propustnost linky mezi PC7 a VDSL klientem PC 9

Profil	**DEFVAL**		**FAST**	
MTU	Rozhraní eth0 [Mbit/s]	Rozhraní tap0 [Mbit/s]	Rozhraní eth0 [Mbit/s]	Rozhraní tap0 [Mbit/s]
128	2	2	10	4
228	8	4	23	8
328	12	6	27	12
428	16	8	28	17
528	17	10	30	20
628	22	12	31	23
728	24	14	31	27
828	23	16	32	31
928	24	18	32	35
1028	25	20	32	37
1128	26	20	33	43
1228	29	23	33	46
1328	27	26	33	50
1428	29	-	33	-
1500	30	-	33	-

Tab. 6: Naměřená propustnost linky v závislosti na velikosti MTU

Realizované zabezpečení využívající VDSL systémy je závislé na zpoždění zapříčiněné vlivem velikosti přenášeného paketu, či prokládáním bitů na DSLAMu. Z těchto důvodů byla proměřena propustnost spojení na lince různých velikostí MTU s krokem 100 bytů, jak udává Tab. 6.

Výsledky jsou zpracovány rovněž ve formě grafu (Graf 1), kde lze pozorovat téměř lineární průběh šifrovaných spojení. U ethernetových zařízení dochází k nejvyššímu nárůstu rychlostí do poloviny velikosti MTU.

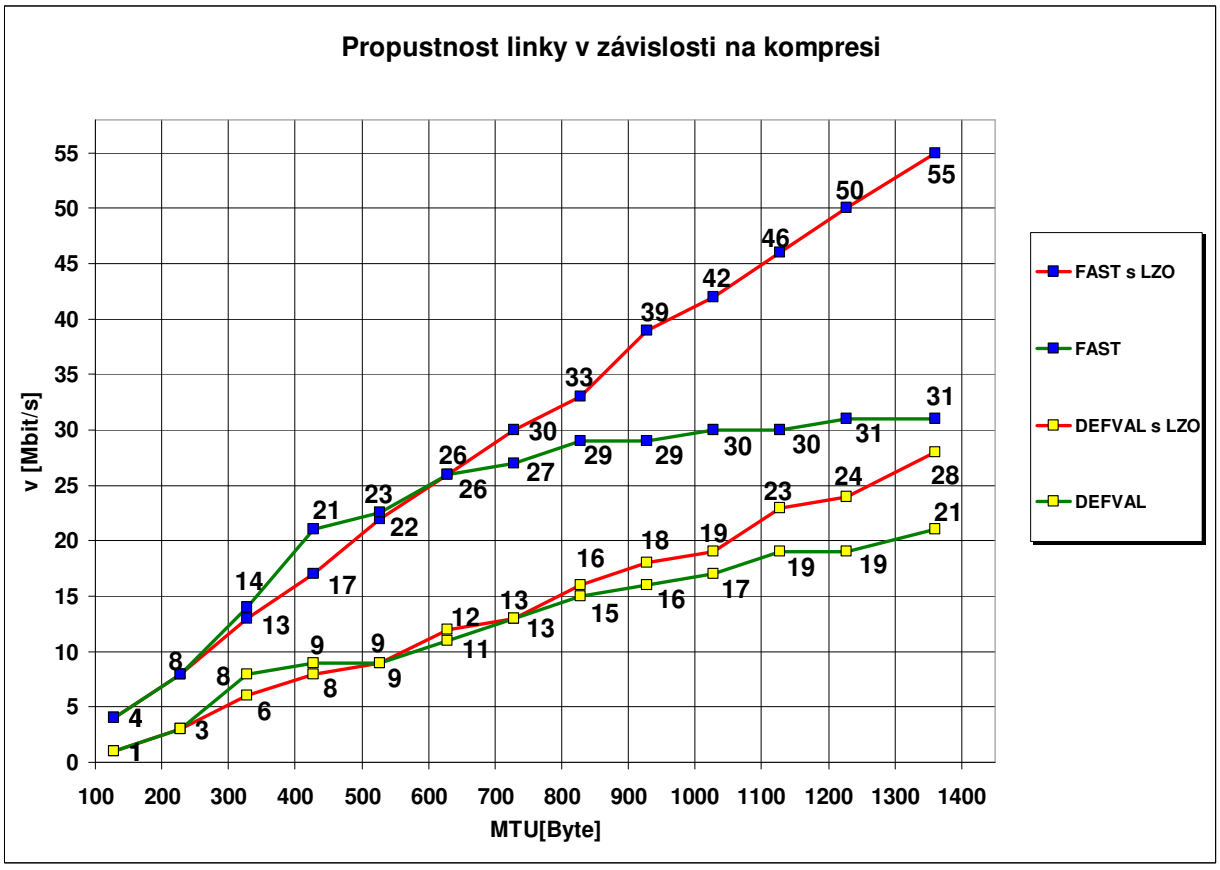


Graf 1: Nárůst rychlostí v závislosti na MTU

Vzhledem k naměřené rychlosti 58 Mbit/s šifrovaného přenosu FAST profilu, uvedené v tabulce 4, je otestován vliv LZO komprese na šifrovaný přenos dat. Měření opětovně probíhalo zasíláním dat s postupně zvyšující se velikostí MTU v možnostech testování programem Iperf. Průběh měření zobrazuje Tab. 7, kde byl vliv komprese zjišťován opět v rámci obou VDSL profilů. Graf 2 znázorňuje přehledněji tuto oblast měření, kde lze pozorovat nárůst rychlostí od 700 bytové MTU u obou profilů, kde dochází k odpoutání kompresních od nekompresních průběhů.

Profil	DEFVAL		FAST	
MTU	S kompresí [Mbit/s]	Bez komprese [Mbit/s]	S kompresí [Mbit/s]	Bez komprese [Mbit/s]
128	1	1	4	4
228	3	3	8	8
328	6	8	13	14
428	8	9	17	21
528	9	9	22	23
628	12	11	26	26
728	13	13	30	27
828	16	15	33	29
928	18	16	39	29
1028	19	17	42	30
1128	23	19	46	30
1228	24	19	50	31
1361	28	21	55	31

Tab. 7: Propustnost VPN spojení v závislosti na kompresi



Graf 2: Nárůst rychlostí při vlivu komprese

3.5. OpenVPN mód server - klient

K tomuto spojení je zapotřebí nakonfigurovaný server, vlastnící veřejnou IP adresu. Na této adrese server poslouchá a čeká na připojení klientů. Po připojení klienta k serveru obě strany vytvoří šifrovaný kanál pro komunikaci. Proběhne-li autentizace klienta, dostane klient IP adresu a stává se součástí sítě. Veškerá komunikace klienta jde nadále přes server a tím je zajištěna bezpečnost dané soustavy.

K vybudování je potřeba vlastních certifikátů. Ty mohou být vytvořené známou certifikační autoritou (obvykle placené), nebo lze vytvořit klientům své vlastní certifikáty pomocí nainstalovaných skriptů. Certifikát autority bude podepsán sám sebou, tzv. self-signed certifikát. [4]

3.5.1. Konfigurace klientských stanic

Pro připojení klientů ke stanici slouží následující postup, zahrnující konfiguraci stanic a vytvoření potřebných certifikátů.

Kvůli možné aktualizaci balíku je dobré si skripty pro tvorbu certifikátů zkopírovat do složky */etc/openvpn/*, což je hlavní složka vlastních specifikací budování VPN, v níž se budou nacházet veškeré nezbytné soubory. Příkazový řádek terminálu:

mkdir /etc/openvpn/easy-rsa/

cp –r /usr/share/doc/openvpn/examples/easy-rsa/2.0/ /etc/openvpn/easy-rsa/*

chmod 600 /etc/openvpn/easy-rsa/

Pro nastavení výchozích hodnot k tvorbě certifikátů je nutno upravit soubor */etc/openvpn/easy-rsa/vars* do následující podoby.

```
export KEY_SIZE=2048
export KEY_COUNTRY="CZ"
export KEY_PROVINCE="CZ"
export KEY_CITY="OSTRAVA"
export KEY_ORG="VSB-TUO"
export KEY_EMAIL="me@myhost.mydomain"
```

Aktivace proměnných a následná generace klíčů:

cd /etc/openvpn/easy-rsa/

. ./vars

./clean-all *//vymazání vzorových klíčů*

./build-ca *// vytvoření certifikační autority*

```
Country Name (2 letter code) [CZ]:
State or Province Name (full name) [CZ]:
Locality Name (eg, city) [OSTRAVA]:
Organization Name (eg, company) [VSB-TUO]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [VSB-TUO CA]:
Name []:
Email Address [me@myhost.mydomain]:
```

Takto vygenerovaný 2048 bitový RSA privátní klíč se uložil do souboru *ca.key*.

./build-key-server server

```
Country Name (2 letter code) [CZ]:
State or Province Name (full name) [CZ]:
Locality Name (eg, city) [OSTRAVA]:
Organization Name (eg, company) [VSB-TUO]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [server]:
Name []:
Email Address [me@myhost.mydomain]:
```

Výsledný výpis z terminálu u verifikační autority by měl obsahovat shodné hodnoty jako i pro server, u kterého je možno doplnit o kontrolní heslo:

```
A challenge password []:
An optional company name []:
```

Dále se provede kontrola žádosti zda se jedná o platná data.

Takto vygenerovaná data podepíše certifikační stanice a vznikne vygenerovaný 2048 bitový RSA privátní klíč, který se uložil do souboru *server.key*. Certifikát má platnost 3650 dní a jedná se o self-signed certifikát. Využívá se konfigurace z */etc/openvpn/easy-rsa/openssl.cnf*.

Obdobně se vytvoří i certifikáty pro všechny klienty, kde vygenerovaný 2048 bitový RSA privátní klientský klíč se uloží do souboru *client1.key*:

./build-key client1 *//vytvoření klientského certifikátu*

./build-key-pass client1 *//vytvoření klientského certifikátu chráněného heslem*

./build-dh *//vytvořit Diffie-Hellman parametry*

Vygenerované soubory jsou nyní uloženy ve složce */etc/openvpn/easy-rsa/keys.* Soubory *client1.crt*, (*client1.csr)*,*client1.key* a *ca.crt* se musí bezpečnou formou dopravit do */etc/openvpn/* na

stanici klienta. Do stejnojmenné složky serveru se zkopírují soubory *ca.crt, server.crt, server.key, dh2048.pem*. Dále je vhodné souborům na serveru přidělit přístupová práva pouze pro roota.

V tuto chvíli jsou patřičné certifikáty na obou stanicích a zbývá už jen přistoupit na konfiguraci souborů VPN na straně serveru a klienta. Jedná se o stěžejní soubory budované privátní sítě s koncovkou *.conf*, které mohou mít následující podobu:

Server.conf

```
mode server                                          # režim mód server
tls-server                                           # SSL/TLS spojení
port 1194                                            # zvolený port
proto tcp-server                                     # TCP komunikace
dev tap0                                             # TUN/TAP virtuální zařízení
ifconfig 192.168.0.8 255.255.255.0                   # adresa serveru
ifconfig-pool 192.168.0.10 192.168.0.15 255.255.255.0 # rozsah adres přidělované klientům
#duplictate-cn                                       # současné přihlášení klientů se
                                                       stejným certifikátem

ca /etc/openvpn/ca.crt                               # certifikát CA
cert /etc/openvpn/server.crt                         # certifikát serveru
key /etc/openvpn/server.key                          # klíč serveru
dh /etc/openvpn/dh2048.pem                           # Diffie-Hellman parametry
#log-apend /var/log/openvpn.log                      # parametry záznamů
status /var/run/vpn.status 10                        # ukládání stavu OpenVPN
keepalive 10 120                                     # udržování spojení
comp-lzo                                             # komprese LZO
verb 3                                               # četnost informovanosti od 0-11
#user nobody                                         # uživatel
#group nobody                                        # skupina
```

client1.conf

```
remote 20.0.0.3                                      # jméno nebo IP adresa serveru
tls-client
port 1194
proto tcp-client
dev tap0
```

#pull # stažení konfigurace ze serveru (push)

ifconfig 192.168.0.10 255.255.255.0

ca /etc/openvpn/ca.crt # certifikát CA

cert /etc/openvpn/client1.crt # certifikát klienta

key /etc/openvpn/client1.key # klíč klienta

mute 10 # tlumení záznamu

#log-apend /var/log/openvpn.log

status /var/run/vpn.status 10

comp-lzo

verb 3

#user nobody

#group nobody

Tab. 8 shrnuje potřebné konfigurační soubory a jejich specifikaci pro spojení server – klient. Klíč certifikační autority je umístěn na serveru, jelikož se jedná o vlastnoručně podepsaný certifikát stanice. Autentizace spojení je uvedena v Příloze 3. [6]

Soubor	Umístění	Funkce	Tajný
vpn.conf	server + klienti	Konfigurační soubor	NE
ca.crt	server + klienti	Certifikát CA	NE
ca.key	pouze CA (server)	Klíč CA	ANO
dh2048.pem	server	Diffie-Helman parametry	NE
server.crt	server	Certifikát serveru	NE
server.key	server	Klíč serveru	ANO
client1.crt	klient1	Certifikát klienta	NE
client1.key	klient1	Klíč klienta	ANO

Tab. 8: Přehled souborů pro konfiguraci [6]

3.5.2. Propustnost linky v režimu server - klient

Dle konfigurace uvedené v kapitole 3.5, byl otestován provoz v režimu server - klient opět pomocí programu Iperf. Tab. 9 zaznamenává maximální rychlosti naměřené mezi stanicemi VDSL klientů opětovně ve třech režimech testování, a to při profilu DEFVAL.

Průměrné hodnoty paketů přenesených za sekundu byly stanoveny z programu Wireshark při reálném testování spojení. Toto současné monitorování zařízení poukazuje na důležitost komprese, při kterém dochází u virtuálního adaptéru na desetinásobně více paketů, než vykazuje adaptér ethernetový.

Tab. 10 zachycuje totožnou strukturu měření, ovšem testovanou pomocí latence s neprokládáním bitů u profilu FAST, nastaveného shodně na portech DSLAMu.

	Zařízení	Pakety/s	Mbit/s
Nešifrované	eth0	4100	29
OpenVPN s LZO kompresí	eth0	1100	51
	tap0	10000	
OpenVPN bez komprese	eth0	2400	17
	tap0	2300	

Tab. 9: Propustnost linky profilu DEFVAL

	Zařízení	Pakety/s	Mbit/s
Nešifrované	eth0	4400	33
OpenVPN s LZO kompresí	eth0	1500	85
	tap0	14000	
OpenVPN bez komprese	eth0	4400	30
	tap0	4370	

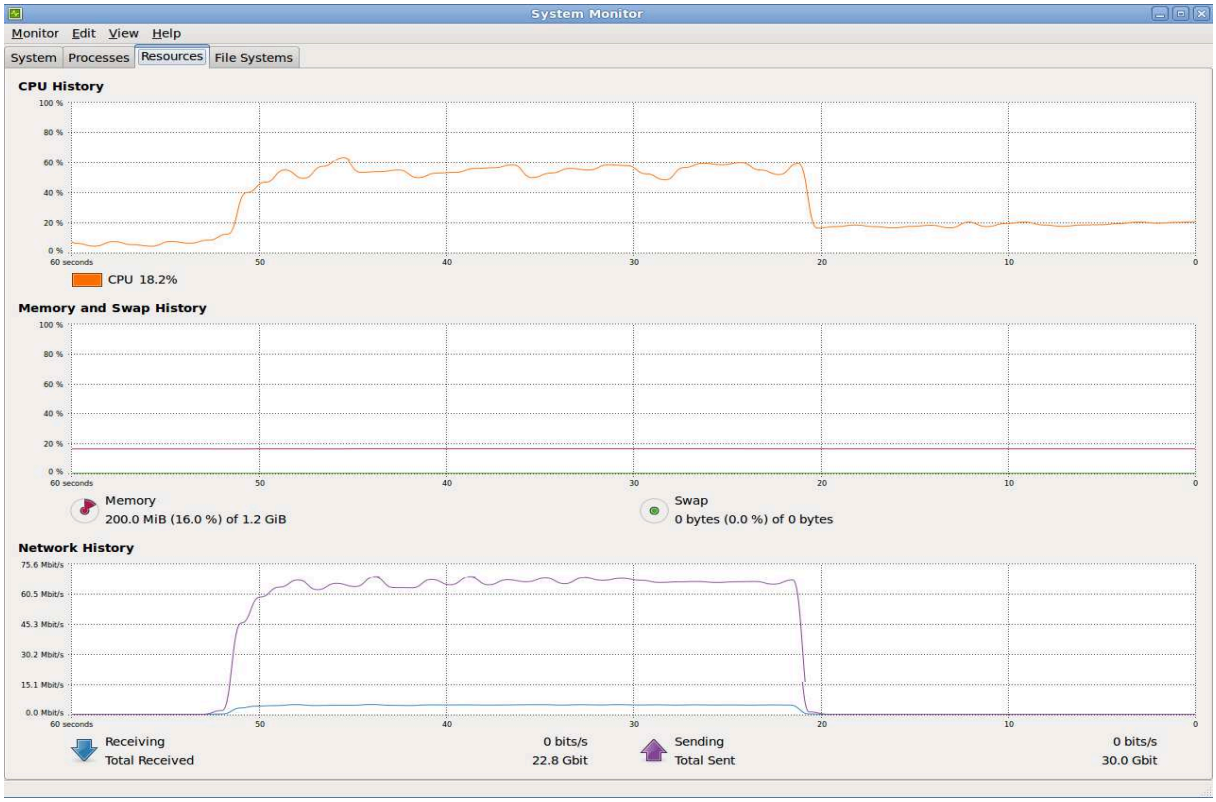
Tab. 10: Propustnost linky profilu FAST

3.6. Využití jednotky CPU

Vybudované šifrované VPN spojení s mnohdy volitelnou kompresí je značně náročné na výpočty počítače. Tab. 11 vyjadřuje vytíženost procesoru stanice při reálném testování přenosu dat. Hodnoty jsou určeny pomocí System monitoru, který se nachází v primární nabídce OS každé stanice na učebně N312. Obr.12 zachycuje uživatelské prostředí měřícího softwaru na klientské stanici.

		Využití CPU		
		Mezi směrovači	Mezi klienty	
			DEFVAL	FAST
Nešifrovaný	Jednostranný	**30 %**	**20 %**	**18 %**
	Oboustranný	40 %	27 %	25 %
		40 %	27 %	25 %
Šifrované OpenVPN s LZO	Jednostranný	**70 %**	**40 %**	**55 %**
	Oboustranný	60 %	45 %	60 %
		60 %	45 %	60 %
Šifrované OpenVPN	Jednostranný	**70 %**	**40 %**	**40 %**
	Oboustranný	80 %	45 %	55 %
		70 %	45 %	55 %

Tab. 11: Vytíženost procesoru



Obr. 12: System monitor stanice

4. Závěr

Teoretická část bakalářské práce je věnována nejen technologii VDSL2, ale i charakteristice předchozího vývoje, popisu funkce použité modulace, standardizovaných profilových skupin, nebo průběhu zapouzdření do rámců. Dále je popsán DSLAM, coby nezbytný prvek, přes který prochází veškerý proud a chod dat klientů. Pro návrh a správnou funkčnost zabezpečení je tento úvod do VDSL nezbytný k prvotnímu pochopení vysokorychlostní technologie a jejího následného testování. Zbývající prostor z teoretické části je již věnován problematice datových přenosů, potenciálních hrozeb a opatřením proti nim. Virtuální privátní síť, která je zde uplatněna, podrobně rozepisuje a znázorňuje klady a druhy úrovní zabezpečení. Popsaná veřejně dostupná OpenVPN metoda pracuje nezávisle na platformě, kde nabízí jednoduchou konfiguraci základního šifrovaného tunelu, nebo režimu server - klient, podporující ověření komunikujících stran pomocí vzájemné výměny certifikátů.

V praktické části je nejprve uvedena postupná konfigurace aktivních prvků pro sestavení sítě. Na straně DSLAMu byly vytvořeny dva profily, DEFVAL a FAST, mající shodnou frekvenční šířku 12 MHz, ovšem u FAST profilu s latencí bez prokládání bitů. Veškeré příkazy a konfigurace jsou navrženy na stanice učebny N312, na kterých se nachází verze Ubuntu OS Linux.

Na aktivní VDSL síť je následně navržen postup vytvoření šifrovaného tunelu mezi klienty. Spuštěním VPN vznikne virtuální ethernet adaptér tap0, vlastnící odlišnou IP adresu podsítě od eth0. Na tap0 zařízení je veškerý provoz dat šifrován vygenerovaným privátním klíčem stanice. Komunikace probíhá na zvoleném protokolu UDP, do kterého jsou zapouzdřena data a následně na tap0 rozbalena.

Takový proces musí být závislý na výpočtech, respektive na čas stanic klientů. Testování propustnosti linky přenosu dat bylo uskutečněno programem Iperf, a pro nezávislost ověřeno i programem Netperf. Měřením byly nejdříve stanoveny výchozí hodnoty bez VDSL technologie (Schéma 2 str. 20). Přenos šifrovaným tunelem byl pomalejší o 10 Mbit/s, než mezi ethernetovými adaptéry. Nevyužití komprese představovalo na šifrovaném tunelu úbytek rychlosti o 27 Mbit/s.

Z těchto poznatků byl následně otestován šifrovaný i nešifrovaný provoz VDSL uživatelů, v kombinacích na zvoleném profilu DSLAMu. Neprokládaný přenos dat FAST profilu byl rychlejší, než veškeré naměřené kombinace profilu DEFVAL. U FAST profilu šifrovaný tunel vykazoval rychlost dvojnásobnou. Tato závratná rychlost je dána vlivem nastavené komprese LZO, která výpočetně operuje nad daty v reálném čase a v kombinaci s VDSL vytváří výtečné zabezpečené vysokorychlostní spojení.

Nejen z důvodu vynikajících hodnot rychlostí byl následně otestován průběh přenosové rychlosti v závislosti na volitelném MTU rámce. Rozdíl s využitím komprese byl patrný z průběhů (Graf 2, str. 25) testování spojů mezi VDSL klienty. Jev komprese se začal uplatňovat již od poloviny MTU.

U VDSL systémů průběh nárůstu MTU u šifrovaného tunelu s kompresí oproti běžnému ethernetovému spoji již nebyl tak zřejmý (Graf 1, str. 24). Pro FAST profil je skutečně platné, aby zabezpečený přenos podléhal kompresi, jelikož od poloviny MTU dochází k navyšování rychlostí až do konečného rozdílu 25 Mbit/s. Zato u průběhů DEFVAL profilu vykazuje tunel s kompresí pomalejší nárůst hodnot, a v konečném důsledku je téměř shodný s ethernetovým. Tento vývoj je spojen s prokládáním bitů na DSLAMu, časem nezbytným k zapouzdření rámců do VPN tunelu i řadou dalších úkonů spojení.

Monitorování vytíženosti procesoru naznačilo dvojnásobné vytížení CPU stanice vlivem šifrování. Mezi VDSL klienty měl vliv na CPU zvolený přenosový profil, než-li komprese LZO.

Cílem této práce bylo zabezpečení přenosů dat v síti. Poznatky z ní lze uplatnit pro reálný návrh vlastní budované sítě, nebo jako výukový materiál vhodný pro vytvoření laboratorního měření. Konfigurace OpenVPN na stanicích klientů na VDSL systémech vytvořilo neomezující a snadno implementované zabezpečení, podporující vynikající přenosové rychlosti. Nemalou výhodou zabezpečení OpenVPN, která pracuje mezi transportní a aplikační vrstvou TCP/IP, je adaptace na nejen zde navržené technologii.

Literatura

[1] *IEEE 802 LAN/MAN Standards Committee*: EoVDSL [online]. 3 July 2001 [cit. 2012-04-19]. Dostupné z: http://www.ieee802.org/3/efm/public/jul01/presentations/mizrahi_1_0701.pdf

[2] ICT REGULATION TOOLKIT. VDSL2: *The Ideal Access Technology for Delivering Video Services Revision 2* [online]. 2006 [cit. 2012-04-19]. Dostupné z: http://www.ictregulationtoolkit.org/en/document.2957.pdf

[3] JAREŠ, P. *Access server*: *Vektorová modulace DMT* [online]. 17. 01. 2007 [cit. 2012-04-18]. Dostupné z: http://access.feld.cvut.cz/view.php?nazevclanku=vektorova-modulace% 20dmt &cisloclanku=2007010002

[4] KRČMÁŘ, Petr. *Linux: postavte si počítačovou síť.* 1. vydání. Praha: Grada, 2008, 182 s. ISBN 978-80-247-1290-1.

[5] OBERHUMER, Markus F.X.J. *Oberhumer.com*: *LZO Documentation* [online]. vyd. 2.06. 12 Aug 2011 [cit. 2012-04-18]. Dostupné z: http://www.oberhumer.com/opensource/lzo/lzodoc.php

[6] *OpenVPN - Open Source VPN: HOWTO* [online]. 2002-2008 [cit. 2012-04-27]. Dostupné z: http://openvpn.net/index.php/open-source/documentation/howto.html

[7] *OpenVPN - Open Source VPN*: *Security Overview* [online]. 2002-2012 [cit. 2012-04-18]. Dostupné z: http://openvpn.net/index.php/open-source/documentation/security-overview.html

[8] PUŽMANOVÁ, Rita. *DSL.cz: Dramatický vývoj DSLAM (první část)* [online]. 29.06.2004 [cit. 2012-04-19]. Dostupné z: http://www.dsl.cz/clanek/15-dramaticky-vyvoj-dslam-prvni-cast

[9] PUŽMANOVÁ, Rita. *DSL.cz: Dramatický vývoj DSLAM (druhá část)* [online]. 08.07.2004 [cit. 2012-04-19]. Dostupné z: http://www.dsl.cz/clanek/19-dramaticky-vyvoj-dslam-druha-cast

[10] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z.* 1. Vydání. Praha: Computer Press, 1998, 446 s. ISBN 80-7226-098-7.

[11] PUŽMANOVÁ, Rita. *Širokopásmový Internet: přístupové a domácí sítě.* 1. vydání. Brno: Computer Press, 2004, 377 s. ISBN 80-251-0139-8.

[12] ŠILHAVÝ, Pavel. *Elektrorevue: Modulace DMT (Discrete MultiTone)* [online]. 2001 [cit. 2012-04-19]. Dostupné z: http://www.elektrorevue.cz/clanky/01006/index.html

[13] ŠIMÁK, Boris, Jiří VODRÁŽKA a Jaroslav SVOBODA. *Digitální účastnické přípojky xDSL: Díl 1. - Metody přenosu, popis přípojek HDSL, SHDSL, ADSL, VDSL.* 1.vydání. Praha: Sdělovací technika, 2005, 141 s. ISBN 80-86645-07-X.

[14] TESTCOM: *Vysokorychlostní přístup ke službám elektronických komunikací* [online]. Březen 2006 [cit. 2012-04-28]. Dostupné z: http://www.testcom.cz/pdf/vyzkum/Vysokorychlostni_pristup_ke_sluzbam.pdf

[15] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí.* Vyd. 1. Brno: CP Books, 2005, 338 s. ISBN 80-251-0417-6.

[16] VODRÁŽKA. *Access server*: *Druhá generace VDSL2* [online]. 30. 11. 2005 [cit. 2012-04-18]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2005093001

[17] Www.SAMURAJ-cz.com: *VLAN - Virtual Local Area Network* [online]. 02.06.2007 [cit. 2012-04-18]. Dostupné z: http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

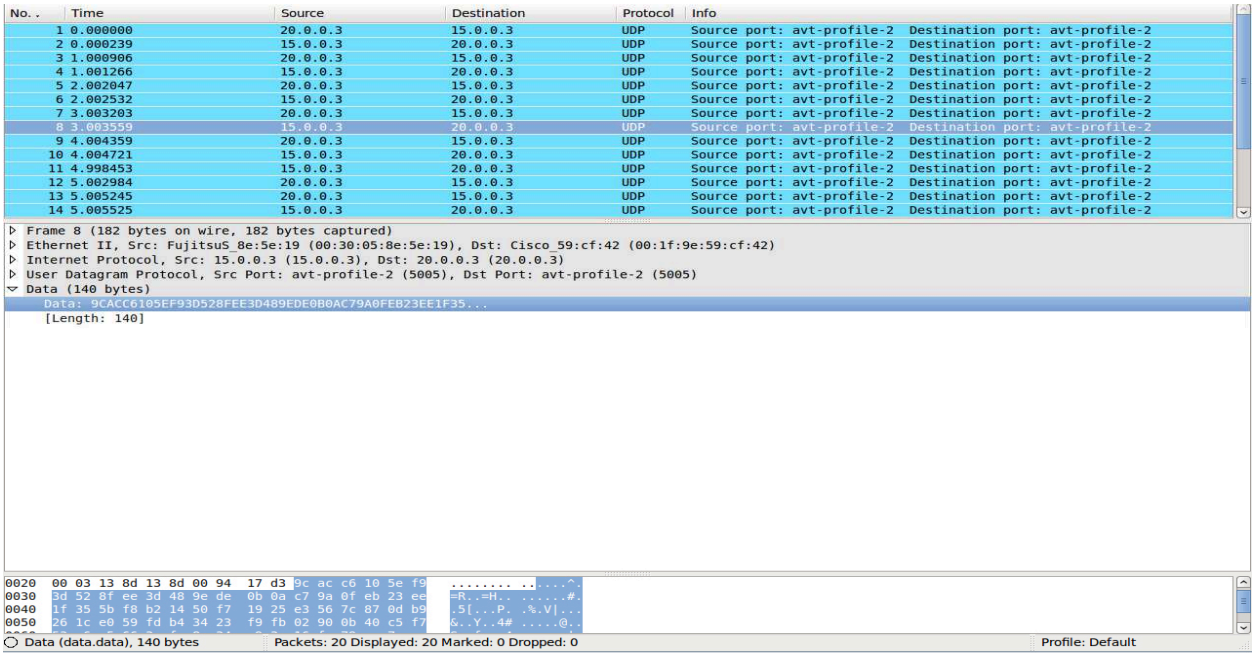
[18] ZIMEK, Michal. *Přenos dat v prostředí digitálních účastnických vedení* [online]. Ostrava, 2011 [cit. 2012-04-28]. 38 s. Dostupné z: http://dspace.vsb.cz/handle/10084/87459. Bakalářská práce. Vysoká škola báňská - Technická univerzita Ostrava.

[19] *ZYXEL Communications Corp: P-870MH-C1*[online]. 2012 [cit. 2012-04-18]. Dostupné z: http://www.zyxel.com/products_services/p_870mh_c1.shtml?t=p

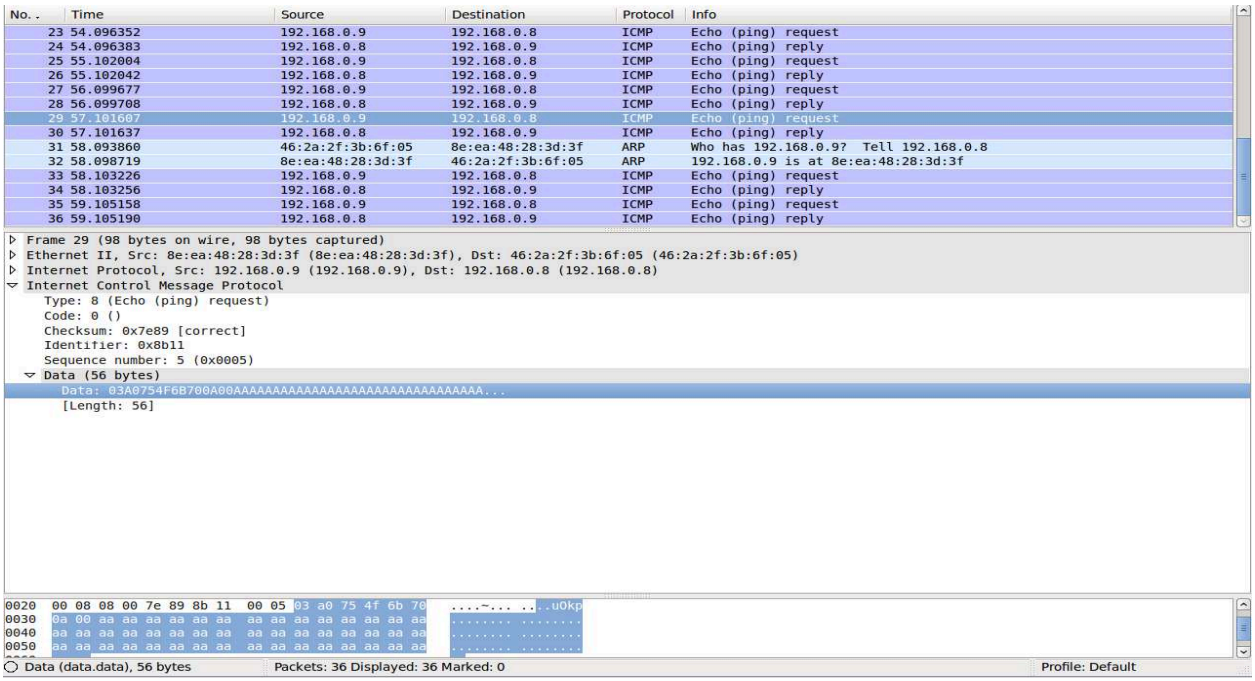
Seznam příloh

Příloha č. 1 – Zachycení provozu

Náhledy, pořízené na eth0 rozhraní programem Wireshark, zachycují přenos paketů obsahující sekvenci znaků „A“. Na Obr. 1 je zobrazen šifrovaný přenos paketů. Obr. 2 přestavuje standardní průběh spojení s nezašifrovanými daty.



Obr. 1: Šifrované spojení



Obr. 2:Odchycení nešifrovaných paketů

Příloha č. 2 – Výpis z terminálu programu Iperf

Zde je uveden výpis z terminálu na straně Iperf klienta (PC 9). Měření je v rámci nešifrovaného rozhraní eth0 a nastaveného profilu DEFVAL na DSLAMu.

```
root@student-desktop:/home/student# iperf -m -t 30 -i 5 -c 15.0.0.3 -p
6666
------------------------------------------------------------
Client connecting to 15.0.0.3, TCP port 6666
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  3] local 20.0.0.3 port 37382 connected with 15.0.0.3 port 6666
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 5.0 sec  16.1 MBytes  27.0 Mbits/sec
[  3]  5.0-10.0 sec  19.5 MBytes  32.7 Mbits/sec
[  3] 10.0-15.0 sec  16.3 MBytes  27.4 Mbits/sec
[  3] 15.0-20.0 sec  16.8 MBytes  28.1 Mbits/sec
[  3] 20.0-25.0 sec  17.2 MBytes  28.8 Mbits/sec
[  3] 25.0-30.0 sec  17.4 MBytes  29.2 Mbits/sec
[  3]  0.0-30.0 sec    103 MBytes  28.9 Mbits/sec
[  3] MSS size 1448 bytes (MTU 1500 bytes, ethernet)
root@student-desktop:/home/student#
```

Příloha č. 3 – Autorizace OpenVPN spojení v režimu server - klient

Výpis z konzole serveru po spuštění OpenVPN dle konfigurace 3.5:

```
root@student-desktop:/home/student# openvpn --config /etc/openvpn/server.conf
OpenVPN 2.1.0 i486-pc-linux-gnu [SSL] [LZO2] [EPOLL] [PKCS11] [MH] [PF_INET6][eurephia]
  built on Jul 20 2010
Apr 2012 NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to call user-
  defined scripts or executables
Apr 2012 Diffie-Hellman initialized with 2048 bit key
Apr 2012 WARNING: file '/etc/openvpn/server.key' is group or others accessible
Apr 2012 /usr/bin/openssl-vulnkey -q -b 2048 -m <modulus omitted>
Apr 2012 TLS-Auth MTU parms [ L:1576 D:140 EF:40 EB:0 ET:0 EL:0 ]
Apr 2012 TUN/TAP device tap0 opened
Apr 2012 TUN/TAP TX queue length set to 100
Apr 2012 /sbin/ifconfig tap0 192.168.0.5 netmask 255.255.255.0 mtu 1500 broadcast
  192.168.0.255
Apr 2012 Data Channel MTU parms [ L:1576 D:1450 EF:44 EB:135 ET:32 EL:0 AF:3/1 ]
Apr 2012 Listening for incoming TCP connection on [undef]
Apr 2012 Socket Buffers: R=[87380->131072] S=[16384->131072]
Apr 2012 TCPv4_SERVER link local (bound): [undef]
Apr 2012 TCPv4_SERVER link remote: [undef]
Apr 2012 MULTI: multi_init called, r=256 v=256
Apr 2012 IFCONFIG POOL: base=192.168.1.1 size=11
Apr MULTI: TCP INIT maxclients=1024 maxevents=1028
Apr Initialization Sequence Completed
```

Po úspěšném nakonfigurování a spuštění klienta se provede mimo jiné výměna certifikátů a dohoda šifrovacích algoritmů. Výpis z konzole serveru:

```
Apr 2012 MULTI: multi_create_instance called
Apr 2012 Re-using SSL/TLS context
Apr 2012 LZO compression initialized
Apr 2012 Control Channel MTU parms [ L:1576 D:140 EF:40 EB:0 ET:0 EL:0 ]
Apr 2012 Data Channel MTU parms [ L:1576 D:1450 EF:44 EB:135 ET:32 EL:0 AF:3/1 ]
Apr 2012 Local Options hash (VER=V4): '3e6d1056'
Apr 2012 Expected Remote Options hash (VER=V4): '31fdf004'
Apr 2012 TCP connection established with [AF_INET]20.0.0.3:60086
Apr 2012 Socket Buffers: R=[131072->131072] S=[131072->131072]
Apr 2012 TCPv4_SERVER link local: [undef]
Apr 2012 TCPv4_SERVER link remote: [AF_INET]20.0.0.3:60086
Apr 2012 20.0.0.3:60086 TLS: Initial packet from [AF_INET]20.0.0.3:60086, sid=c5ac164b
18432e72
Apr 2012 20.0.0.3:60086 VERIFY OK: depth=1, /C=CZ/ST=CZ/L=OSTRAVA/O=VSB-TUO/CN=VSB-
TUO_CA/emailAddress=me@myhost.mydomain
Apr 2012 20.0.0.3:60086 VERIFY OK: depth=0, /C=CZ/ST=CZ/L=OSTRAVA/O=VSB-
TUO/CN=client1/emailAddress=me@myhost.mydomain
Apr 2012 20.0.0.3:60086 WARNING: 'ifconfig' is present in remote config but missing in
local config, remote='ifconfig 192.168.1.0 255.255.255.0'
Apr 2012 20.0.0.3:60086 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Apr 2012 20.0.0.3:60086 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC
authentication
Apr 2012 20.0.0.3:60086 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Apr 2012 20.0.0.3:60086 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC
authentication
Apr 2012 20.0.0.3:60086 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 2048
bit RSA
Apr 2012 20.0.0.3:60086 [client1] Peer Connection Initiated with [AF_INET]20.0.0.3:60086
Apr 2012 client1/20.0.0.3:60086 MULTI: Learn: de:b7:1c:db:68:d8 -> client1/20.0.0.3:60086
```

Zde je uveden záznam a výpis z konzole na straně klienta:

```
root@student-desktop:~# openvpn --config /etc/openvpn/client.conf

Apr 6 2012 OpenVPN 2.1.0 i486-pc-linux-gnu [SSL] [LZO2] [EPOLL] [PKCS11] [MH]
[PF_INET6] [eurephia] built on Jul 20 2010
Apr 6 2012 NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to call user-
defined scripts or executables
Apr 6 2012 WARNING: file '/etc/openvpn/client1.key' is group or others accessible
Apr 6 2012 /usr/bin/openssl-vulnkey -q -b 2048 -m <modulus omitted>
Apr 6 2012 LZO compression initialized
Apr 6 2012 Control Channel MTU parms [ L:1576 D:140 EF:40 EB:0 ET:0 EL:0 ]
Apr 6 2012 TUN/TAP device tap0 opened
Apr 6 2012 TUN/TAP TX queue length set to 100
Apr 6 2012 /sbin/ifconfig tap0 192.168.1.6 netmask 255.255.255.0 mtu 1500 broadcast
192.168.1.255
Apr 6 2012 Data Channel MTU parms [ L:1576 D:1450 EF:44 EB:135 ET:32 EL:0 AF:3/1 ]
Apr 6 2012 Local Options hash (VER=V4): '585399e1'
Apr 6 2012 Expected Remote Options hash (VER=V4): '27a72bb3'
Apr 6 2012 Attempting to establish TCP connection with [AF_INET]15.0.0.3:1194
[nonblock]
Apr 6 2012 TCP connection established with [AF_INET]15.0.0.3:1194
Apr 6 2012 Socket Buffers: R=[87380->131072] S=[16384->131072]
Apr 6 2012 TCPv4_CLIENT link local: [undef]
Apr 6 2012 TCPv4_CLIENT link remote: [AF_INET]15.0.0.3:1194
Apr 6 2012 TLS: Initial packet from [AF_INET]15.0.0.3:1194, sid=7c03e646 345e8792
Apr 6 2012 VERIFY OK: depth=1, /C=CZ/ST=CZ/L=OSTRAVA/O=VSB-TUO/CN=VSB-
TUO_CA/emailAddress=me@myhost.mydomain
Apr 6 2012 VERIFY OK: depth=0, /C=CZ/ST=CZ/L=OSTRAVA/O=VSB-
TUO/CN=server/emailAddress=me@myhost.mydomain
Apr 6 2012 WARNING: 'ifconfig' is present in local config but missing in remote
config, local='ifconfig 192.168.1.0 255.255.255.0'
Apr 6 2012 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Apr 6 2012 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC
authentication
Apr 6 2012 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Apr 6 2012 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC
authentication
Apr 6 2012 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 2048 bit RSA
Apr 6 2012 [server] Peer Connection Initiated with [AF_INET]15.0.0.3:1194
Apr 6 2012 Initialization Sequence Completed
```